NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**THE PRESIDENT HAS NO CLOTHES:
THE CASE FOR BROADER APPLICATION OF RED TEAMING WITHIN HOMELAND SECURITY**

by

A. Bentley Nettles

June 2010

Thesis Advisor:	David Brannan
Second Reader:	Greg Fontenot

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2010	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
The President Has No Clothes: The Case for Broader Application of Red Teaming Within Homeland Security	
6. AUTHOR(S) A. Bentley Nettles	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

Missing in DHS' current gap and vulnerability analysis approach to Red Teaming is the employment of broader decision support Red Teaming—which would provide a strategic assessment tool, assisting the organization in overcoming group thinking and a lack of organizational creativity, while avoiding mirror imaging. DHS, by broadening its use of Red Teaming, will improve its decision-making processes across all levels of homeland security. This research uses a selected case study—identifying and challenging assumptions inherent within TSA's security system, analyzing the problem using an alternative model, and looking at the problem from different perspectives. Combined with evidence and analysis from historical examples, this effort is designed to determine whether decision makers can benefit from Red Teams and Red Team fundamental concepts, and whether these concepts will be effective in assisting DHS and its partners in making better decisions.

America's Homeland Security System is hampered by bureaucratic challenges. The U.S. government must dramatically re-orient itself. America needs to redefine its homeland security approach into a flexible adaptive system. Understanding the U.S. layers of security, and how they interact to defeat the terrorist threat, is as critical as understanding "Red"—what our enemies are doing. Trained Red Teams apply creative thinking, and Red Team fundamentals, challenge the organization's assumptions, provide alternative analysis to the organization's plans, and provide the decision maker with alternative perspectives on the current operating environment. Education on the Red Team Fundamentals should be implemented as mandatory for all homeland security leaders. DHS should: implement decision support Red Teams as part of its force structure; implement joint enterprise Red Teams between its own agencies and facilitate joint enterprise Red Teams between DHS and other security agencies, entities and partners; and implement Red Team integration into the Homeland Security technology approval process.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Red Team, Homeland Security, Department of Homeland Security, Transportation Safety Administration	95
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release: distribution is unlimited

THE PRESIDENT HAS NO CLOTHES: THE CASE FOR BROADER APPLICATION OF RED TEAMING WITHIN HOMELAND SECURITY

A. Bentley Nettles
Colonel, United States Army
B.A., Texas A&M University, 1985
J.D. South Texas College of Law, 1987

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2010**

Author: A. Bentley Nettles

Approved by: David Brannan
Thesis Advisor

COL (R) Gregory Fontenot
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Missing in DHS' current gap and vulnerability analysis approach to Red Teaming is the employment of broader decision support Red Teaming—which would provide a strategic assessment tool, assisting the organization in overcoming group thinking and a lack of organizational creativity, while avoiding mirror imaging. DHS, by broadening its use of Red Teaming, will improve its decision-making processes across all levels of homeland security. This research uses a selected case study—identifying and challenging assumptions inherent within TSA's security system, analyzing the problem using an alternative model, and looking at the problem from different perspectives. Combined with evidence and analysis from historical examples, this effort is designed to determine whether decision makers can benefit from Red Teams and Red Team fundamental concepts, and whether these concepts will be effective in assisting DHS and its partners in making better decisions.

America's Homeland Security System is hampered by bureaucratic challenges. The U.S. government must dramatically re-orient itself. America needs to redefine its homeland security approach into a flexible adaptive system. Understanding the U.S. layers of security, and how they interact to defeat the terrorist threat, is as critical as understanding "Red"—what our enemies are doing. Trained Red Teams apply creative thinking, and Red Team fundamentals, challenge the organization's assumptions, provide alternative analysis to the organization's plans, and provide the decision maker with alternative perspectives on the current operating environment. Education on the Red Team Fundamentals should be implemented as mandatory for all homeland security leaders. DHS should: implement decision support Red Teams as part of its force structure; implement joint enterprise Red Teams between its own agencies and facilitate joint enterprise Red Teams between DHS and other security agencies, entities and partners; and implement Red Team integration into the Homeland Security technology approval process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BDO	Behavior Detection Officers
BDO	Behavior Detection Officers
CIRT	Critical Infrastructure Red Team
DHS	Department of Homeland Security
FAMS	Federal Air Marshals
FAMs	Federal Air Marshals
FFDO	Federal Flight Deck Officer
FFDO	Federal Flight Deck Officer
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
MAAM	Military-Aged Arab Male
NIPP	National Infrastructure Protection Plan
PETN	Pentaerythritol Tetranitrate
QATTs	Qualified Anti-Terrorism Technologies
SAFE	Strategy and Force Evaluation
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration
VIPR	Visible Intermodal Prevention and Response
VIPR	Visible Intermodal Prevention and Response (VIPR)

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I owe a tremendous debt of gratitude to the many people who made this thesis possible. The list begins with my very patient and supportive committee, Dr. Dave Brannan of the Naval Postgraduate School, and Greg Fontenot of the University of Foreign Military and Cultural Studies, Fort Leavenworth, Kansas. Their insight and enthusiasm for an unusual homeland security topic helped shape this project into something that will hopefully shape Homeland Security policy and ensure the future security of the United States. I also wish to thank my editor, Janis Higginbotham, whose extreme patience and persistence during the editing process helped finalize this project.

I also want to thank the Red Teamers I served with first at XVIII Airborne Corps as the unit's first assigned Red Team, then at MNC-I on General. Odierno's staff, and finally at MNF-I as the first Red Team on General Patreaus' staff. The experiences and lessons I learned from them helped me formulate the basis for this thesis.

For their longstanding personal support of this project, I must thank my wife Tracy Nettles and my family. They extended themselves on every personal front so that I could attend this program and complete this thesis. Finally and perhaps above all, I must thank the leadership of the Texas National Guard, who very generously allowed me the opportunity to be away from work to participate in the program and work on this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

We know there are some things
We do not know.

—Secretary of Defense Don Rumsfeld – April 2003

Adversaries currently facing the United States are tougher targets for our intelligence communities than was the Soviet Union.[1] Among the many threats, facing homeland security is the asymmetric threat of terrorism. This terrorism threat can originate form abroad or be homegrown.[2] One reason this new asymmetric threat is very difficult for us to deal with as a nation, is because today's terrorists appear to possess thought processes that are very different from our own. We are not organized or equipped to handle most terrorist threats.[3] This terrorist threat is asymmetric in nature and may originate from a sub national or multinational entity. As a result, the U.S. faces a significant challenge in trying to anticipate how the enemy will act against us.[4]

The Problem Statement: The Red Teaming approach used by the Department of Homeland Security is primarily the gap and vulnerability analysis approach. Physically oriented Red Teams using this approach focus on the ability to defeat security systems in the critical infrastructure arena.[5] Missing in DHS' approach to Red Teaming is the employment of broader decision support to Red Teaming. Broader support would provide strategic assessment while assisting the organization in overcoming group thinking and a lack of

---

[1] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Defense Science Board Task Force, *The Role and Status of DoD Red Teaming Activities* (Washington D.C., September 2003), 1.

[2] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (*New York: W.W. Norton & Company, 2004), 379.

[3] Robert David Steele, "*TAKEDOWN: The Asymmetric Threat to the Nation,"* Joint Forces Quarterly (Winter 1998–99).

[4] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 105.

[5] Richard Alt (Red Team Leader, DHS). Telephone interview, November 17, 2009.

organizational creativity or imagination, while avoiding mirror imaging. Within the Department of Homeland Security, as well as the homeland security community, a void exists in the area of decision support Red Teaming capabilities. This capability is designed to assist leaders in thinking Red when making critical decisions.[6] DHS by broadening its use of Red Teaming from gaps and vulnerability analysis to include strategic decision support Red Teaming, DHS will grow its Red Team capability and improve decision-making processes across the tactical, operational, and strategic levels of homeland security.

Examples: As dawn breaks, a Joint Task Force is steaming towards the Middle East. Recently a rogue Middle Eastern country has been thumbing its nose as UN demands to halt its nuclear enrichment program. The nation has become more and more belligerent, threatening U.S. interests and allies in the region. In response, the U.S. has sent a Joint Task Force to include a carrier group, with amphibious capabilities, in order to intimidate the rogue commander to comply through some arm bending diplomacy. If not, then the U.S. will have increased its military response options, by locating the task force close to the rogue nation. While most nations insist that the international water boundary is 12 miles, the U.S. has maintained that it controls the blue ocean waters and to ensure international navigatibility, the international water boundary is only three miles from the rogue nation's shores.

On day two, the naval flotilla has moved within striking distance of the rogue nation, ignoring the twelve-mile international water boundary. In response, the rogue commander sent out small PT style boats as pickets to pick up, locate the American flotilla, and make darting, harassing runs at the warships. Suddenly, at midnight of the second day, the rogue commander fires upon the Americans. Although not unexpected, the volume of the attack is surprising and quickly overwhelms the task forces defenses. As the sun rises on the third day,

[6] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 364.

the Joint Task Force Commander examines the damage, to find over half of his war ships have been sunk or scuttled with thousands of military personnel, either killed or missing.[7]

How could this happen? How could the greatest military, with all of its superior information-gathering capabilities, misjudge or be surprised by a third-rate military power? Could this be fiction? Not quite. That is precisely what happened during Operation Millennium Challenge. Based upon the notional situation of a rogue nation in the Middle East, the U.S. staged a computer-enhanced exercise involving actual military forces in the field simulating some of the activities, pitting all our information-gathering capabilities and joint operating capabilities against a Red Team, who played the role of the enemy. The only problem is the enemy did not act the way he was supposed to act. Headed by a Vietnam-era, retired Marine Corp General Officer, LTG(R) Paul Van Ripper, the Red Team had its forces communicate by messenger or face-to-face. No phones allowed! This took away the Americans' electronic eavesdropping capability. In response to expected U.S. sorties sent to knock out his long-range rocket capabilities, Van Ripper ordered all his long-range missile assets utilized in a sneak attack, before the U.S. began flight operations. Afterwards, the pentagon claimed this would never have happened. Van Ripper countered that only a fool would attempt to go head to head with the U.S. militarily after Desert Storm and the invasion of Iraq, which showed the world that the U.S. strike capabilities exceeded anyone's imagination. [8] The military focused on the goal of obtaining superior intelligence while communicating large amounts of data—nearly instantaneously—in order to eliminate the fog of war and enable a smaller force, with speed and technology, to achieve decisive results. This similar approach, favoring the use of America's technological advantages, has been adopted in homeland security. Through the increased use of technology, we can close the

[7] Malcom Gladwell, *Blink: The power of thinking without thinking* (New York: Little, Brown and Co., 2007).

[8] D. Longbine, "Red Teaming: Past and Present" (Monograph, School of Advanced Military Studies, Fort Leavenworth, Kansas, 2008), 46.

gap in our vulnerabilities. Reliance upon technology and information to solve a problem is a typical American solution. Yet, despite our technological and information superiority, the enemy continually surprises us.

A. UNDERESTIMATING THE ENEMY

During Operation Iraqi Freedom, LTG Wallace, the V Corps Commander, told reporters, "The enemy we are fighting is a bit different than the one we war-gamed against."[9] LTG Wallace's comment demonstrates that despite the deliberate planning effort before the U.S.-led invasion of Iraq, and the magnificent performance of the coordinated allied and U.S. military effort that resulted in complete dismantling of the Iraqi regime's military between March 20 and May 1, 2003, the effort failed to defeat the true enemy. The nature of the Iraqi regime collapse gave rise to the insurgency that the U.S. and allies continued to fight for almost five years after major combat operations ceased.[10] After defeating the Iraq military, U.S. military planners had assumed that some of the government and military structure would still be in place to assist with the post-conflict stabilization operations. This assumption proved to be wrong, and went unchallenged during the planning process.

In 2001, despite our efforts at deliberate planning for the security of the United States, the terrorists surprised our homeland security apparatus by using planes as weapons of mass destruction. Although our intelligence services envisioned this possibility, we failed to act upon this potential threat. Then again, the terrorists surprised us on December 25, 2009, Flight 253; Al Qaeda used a known but unexpected technique to bypass security defenses by sewing explosives in their operative's underwear and attempting to create a chemical explosive reaction by injecting another chemical into the explosive. The resulting

---

[9] Michael Gordan and Bernard Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon Books, Random House Inc. 2006), 311.

[10] Stephen T. Hosmer, "*Why the Iraqi Resistance to the Coalition Invasion Was So Weak,"* (Monograph, Rand: Air Force Project, 2007), 2.

explosion was intended to destroy the airplane, killing its passengers, crew, and potentially many more on the ground at the Detroit airport.

B. THE PROBLEM WITH SURPRISE

Surprise is a symptom of the systemic problem within the decision-making process and intelligence assessment involved in homeland security, resulting from failure of imagination or lack of imagination, reflected in the miscalculation created from projections of one's own values unto the enemy's actions and intentions.[11] Our inability to recognize the weaknesses within our plans, security systems, and underestimating the intentions and capabilities of our enemies stems from this lack of imagination.[12] This lack of imagination has basic penalties for both individuals and institutions. The basic penalties for lack of imagination are the failure to recognize danger—with a corresponding increase of vulnerability to strategic surprise, and a narrowing of "the menu of policy options."[13] In Chapter 11 of the 9/11 Commission Report, "Foresight—and Hindsight," the Commission considered "the 9/11 attacks revealed four kinds of failures on behalf of the U.S. Government. Failures: in imagination, policy, capabilities and management."[14] Of these four types, they considered imagination failure to be the most grave. The Commission attributed the failure to understand the danger America faced to the inability to perceive the dangers of Islamic terror, to identify al-Qaida as the enemy, and to anticipate that America's enemies could use commercial passenger airplanes as weapons of mass destruction. Although posed as an open question, the Commission concluded, that: "...the possibility [of a suicide aircraft hijacking] was imaginable, and

[11] James Wirtz, "Miscalculation, Surprise and American Intelligence After the Cold War," *International Journal of Intelligence and Counterintelligence* 5, no. 1, 1991, 5.

[12] Ibid., 5.

[13] J. Fishman, "The Need for Imagination in International Affairs," *Israel Journal of Foreign Affairs III* (2009), 3.

[14] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 356.

imagined."[15] The consequences of this failure: “Nearly three thousand people died in the terrorist attacks of September 11, 2001. In Lower Manhattan, on a field in Pennsylvania, and 103 along the banks of the Potomac, American’s died as a result of this imagination failure.”[16] It is wrong to think of imagination only as a child’s pastime. If a government’s ability to recognize a “first-order threat” and to choose an appropriate defensive response depends even partially on imagination, then being able to exploit the lessons of historical experience and to make creative use of this gift is really a matter of strategic importance. This necessary government skill is even more important if the adversary seeks to inflict (and is prepared to accept) great losses in order to achieve its ends.[17]

C. FAILURE OF IMAGINATION

Five years after the 9-ll commission finalized its report and submitted recommendations, the criticism in the commission’s findings still echo: “We believe the 9/11 attacks revealed four kinds of failures: 1) in imagination, 2) policies, 3) capabilities, and 4) management.[18] The commission concluded that the intelligence community had failed to analyze how an aircraft, hijacked or explosion-laden, could be used as a weapon. They failed to do the kind of analysis desperately needed from the enemy’s perspective (“Red Team” analysis); despite the fact suicide terrorism had become a principal tactic of Middle Eastern terrorist.[19] “Imagination is not a gift usually associated with bureaucracies,”[20] so how does DHS ensure that there are no repeat failures in imagination?

---

[15] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 352.

[16] Ibid., 109.

[17] Ibid., 106.

[18] Ibid., 107.

[19] Ibid., 347.

[20] Ibid., 346.

D. SECURITY CHALLENGES

Predicting and anticipating what the enemy will do is an extremely difficult task. The security environment facing the U.S. homeland is dynamic and adaptive. Unlike the days of the Cold War, where foreign nation states would exhibit warnings and indications that their military machine was revving up to flex its muscle, our modern-day enemy is a terrorist. The indications that a terrorist is getting ready to act are subtle, and their members are hidden among the general population.[21] Our security response capability has to continually adapt to match this changing operating environment. Because of its investigation results, the 911 Commission Report challenged DHS and the intelligence community to adapt and incorporate Red Teaming.[22] Within the Department of Homeland Security, several agencies have acted upon the 9-11 Commission's recommendations and are implementing Red Teaming. However, no one seems to know exactly how many Red Teams exist, what type of training they have been exposed to, and how exactly they are being utilized.[23] The current Department of Homeland Security Red Team is housed within the Department of Homeland Security Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and is referred to as the Critical Infrastructure Red Team (CIRT).[24] The CIRT is designed to help educate and enhance DHS and National Infrastructure Protection Plan (NIPP) partners' understanding of the threats to Critical Infrastructure and Key Resources by introducing them to a synthesis of operational planning and terrorist-intelligence capabilities through a process of target selection. These capabilities include: 1) Analyzing terrorist targeting choices, 2) providing terrorist planning perspectives, 3) developing simulated

---

[21] R. Poole, "Toward Risk-Based Aviation Security Policy", Discussion Paper No. 2008-23 (Joint Transport Research Centre (November 2008), 11.

[22] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 347.

[23] Federal, state, and local government representatives (Second DHS Red Team Conference) personal interviews, February 2009.

[24] Alt, *Critical Infrastructure Red Team,* Brochure, undated.

terrorist attack plans, 4) designing and executing tailored tabletop simulations and 5) translating insights obtained from specific operations and exercises useful lessons learned.[25]

Department of Homeland Security's Critical Infrastructure Red Team attempts to replicate the terrorist perspective the security vulnerabilities of a critical infrastructure by identifying a terrorist target selection based on a terrorist threat perspective chosen from a specific threat group, a Universal-Adversary Program profile, or is uniquely constructed from emerging intelligence data. CIRT develops an understanding of the selected adversary's selection criteria in order to replicate its method of target selection. The team utilizes such aspects as a terrorist group's ideology to understand target desirability, its goals to determine desired results of the attack, and its resources and capabilities to determine the attack method, scale, and timeline.[26]

The CIRT provides this outreach program to assist any federal, state, tribal, or local activity, or any critical infrastructure/key resource owner or operator, and tailors the product to the particular need of its security partner. The team operates from the adversary's vantage point and information constraints, without taking advantage of internal DHS intelligence and security insight. Their assessments are based on operationally validated findings through both open-source and on-site reconnaissance (when approved), rather than solely on engineering-based assumptions. CIRT develops its terrorist attack plans in sufficient detail to translate the plans into briefings that can help owners and operators better understand terrorist planning factors and how a terrorist might view individual targets' security, exploiting vulnerabilities it finds.[27]

The CIRT's Red Teaming effort is focused almost entirely on physical Red Teaming, or defeating security processes and procedures to demonstrate

[25] Alt, *Critical Infrastructure.*

[26] Personal Interviews, DHS Red Teaming Conference, February 2009.

[27] Alt, *Critical Infrastructure.*

vulnerabilities in plans, processes, and systems designed to protect critical infrastructure. Currently, CIRT operates primarily as threat emulators, incorporating an attacker defender model to assess vulnerability of our critical infrastructures. The attacker-defender model assesses vulnerability by first assuming that our critical infrastructure will be attacked.[28] The focus of the CIRT program is limited to a specific narrow threat related to specific targets. The DHS Red Team does this very well and performs a valuable service when assessing the vulnerability of a particular critical infrastructure.

This physical and active Red Teaming performed by the CIRT is an essential capability within DHS. However, the broader utilization of Red Teams at the strategic level, and greater understanding and incorporation of Red Team fundamentals by homeland security leaders, is often missing. Adoptions of Red Teaming at the strategic level within DHS will enable it and its partners to become a learning organization. What is missing is Decision Support Red Teaming, or analytical Red Teaming at the strategic level, designed to assist leaders in thinking Red (understanding the enemy's perspective) when making critical decisions. Recently, the Homeland Security Advisory Council to the incoming Secretary of Homeland Security highlighted this deficiency. A mechanism must be developed to enhance leaders' abilities to think like our adversaries, or to look at problems through different lenses and challenge institutional assumptions.[29] Expanding the use of Red Teams beyond the active and tactical focus, and the incorporation of fundamental Red Team concepts by DHS leaders, will help to routinize imagination within Homeland Security.

Despite America's technological advantage, we continue to be surprised by the enemy. The enemy surprised America on 9/11, the enemy surprised America's security forces during operational exercises in the case of GEN Van Ripper's actions and comments during millennium challenge. Finally, the

[28] Gerald Brown et al., "Defending Critical Infrastructure," *Interfaces* 36(6), (2006) 530–544.

[29] Homeland Security Advisory Council, "Top Ten Challenges facing the Next Secretary of Homeland Security" (Washington, D.C., Government Printing Office, September 11, 2008), 12.

American military forces were also surprised during combat operations during operation Iraqi Freedom per the comments of LTG Wallace, that the enemy was not the enemy we planned for.[30] In order to attempt to provide an institutional antidote for surprise, DHS has implemented tactical, security-focused Red Teams through the CIRT. Unfortunately, these teams afford DHS only a small section of the overall benefits that could be enjoyed by creating and implementing a broader application of the Red Team concept and Red Teaming fundamentals.

[30] Bob Kerr, Comment on "Meet the Press: New Combined Arms Center commander discusses Iraq, training, leaders, lessons-learned." Posted August 28, 2003, TRADOC News Service.

II. RED TEAM FOUNDATIONS

To every complex question, there is a simple answer and it is wrong…

—H.L. Mencken

A. UNDERSTANDING RED TEAMING

The literature on Red Teaming specifically related to homeland security or defense is relatively limited and undeveloped. The literature that does exist, for purposes of this research, will be divided into three general categories. The first involves Red Teaming within the Department of Defense (DoD). The second sub area of literature related to Red Teaming explores its development through history. The third sub area of literature involves the issue of Red Teaming as it relates specifically to the way it is executed. The most notable reference to Red Teaming within homeland security literature is the *9-11 Commission Report,* which identifies Red Teaming as a critical element lacking within our homeland security and intelligence structure.[31]

B. DEFINING THE TERM RED TEAM

One area of significant divergence within the literature about Red Teaming is the term itself. "Red Teaming" resists being easily defined, because it is applied in so many different forms to so many different types of problems.[32] Reviewing literature beyond homeland security, the term *Red Team* describes an array of activities. However, throughout the attempts to define the scope of activities that comprise Red Teaming and attempts to identify the varying types of Red Teaming, there appears to be agreement that the overall goal of Red Teaming is to challenge one's own assumptions in order to better understand the

[31] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 352.

[32] Mike McGannon, "Developing Red Team Tactics, Techniques and Procedures," *Red Team Journal,* April 2004).

adversary's perspective and to identify one's own vulnerabilities.[33] Red Teaming typically is used as a peer review process of a concept or proposed course of action.[34] Red Teams can be utilized to look for unexpected scenarios or identify unexpected consequences to a particular approach. It can open a new way of thinking about the security environment, by anticipating and simulating the decision making and behaviors of potential adversaries.[35] America's adversaries will continue to adapt to our security concepts in new and unexpected ways, by emphasizing their own strengths.[36] Red Teaming is beneficial to the security of the United States because it allows us to examine how our enemies view us, so that we can better understand how they evaluate our strengths and weaknesses.[37]

[33] Anna Culpepper, Effectiveness of Using Red Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack, Naval Postgraduate School Master's thesis, September 2004, 9.

[34] Timothy Malone and Reagan Schaupp, "The Red Team: Forging a Well-Conceived Contingency Plan," *Aerospace Power Journal* XVI, no. 2 (Summer 2002), 23.

[35] John F. Sandoz, "Red Teaming: A Means to Military Transformation," *Institute for Defense Analyses Paper P-3580, Log H 00_002905 (*January 2001), 1.

[36] Ibid., 2.

[37] McGannon, "Developing Red Team Tactics, Techniques and Procedures," *The Vanguard*, (Spring 2005), 4.

Figure 1. UFMCS Definition of Red Teaming

Figure 1 represents the University Foreign Military and Cultural Studies (UFMCS) definition of Red Teaming, which emphasizes the use of the Red Team to create an independent capability for the head of the agency to conduct independent and alternative analysis.[38] A trained Red Team can be a value-adding mechanism to the decision maker's analytical process.[39] It assists the decision maker by providing insight to threat perspectives, while also challenging the assumptions and perspectives of the organization.[40] Done successfully, decision support Red Teaming can assist the decision maker by ensuring he or she gets a broader view of the problem, operating environment and

[38] *Red Team Handbook*, version 4, 10.

[39] Ibid., 11.

[40] Ibid.

understanding of vulnerabilities inherent within the analytical process of the decision, due to organizational bias, perspective, and interpretation of the issue to be decided.[41]

Within the Department of the Army, Red Teams accomplish a number of tasks, including identifying how the enemy and other stakeholders think and helping to identify cultural issues involving the enemy and U.S. partners.[42] Although similar within the other services, Red Teams are viewed and employed differently. The air force's definition is more practical of the Red Teaming process, in that Red Teaming is defined as an iterative, interactive process conducted during crisis action planning to assess planning decisions, assumptions, courses of action, processes, and products from the perspective of friendly enemy and outside organizations.[43]

DHS and its agencies and partners have implemented the Red Teaming concept in various ways. The DHS Exercise and Evaluation program defines a Red Team as a group of subject matter experts with various appropriate disciplinary backgrounds that provides an independent peer review of plans and processes, acts as a devil's advocate, and knowledgably role-plays the enemy using a controlled, realistic, interactive process during operations planning, training, and exercising.[44] For purposes of this study, I have adopted the definition used by Dr. Kirkpatrick and her team, which is broadly inclusive of Red Teaming activities that serve as surrogate adversaries or competitors of the enterprise—devil's advocates, independent sources of judgment of the

---

[41] Meehan, "Red Teaming for Law Enforcement," *The Police Chief Magazine* 74, no. 2 (Alexandria, Virginia, February 2007), 1.

[42] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Defense Science Board Task Force, *The Role and Status of DoD Red Teaming Activities*, (Washington D.C., September 2003), 3.

[43] *Red Team Handbook*, version 4, 24.

[44] Meehan, "Red Teaming for Law Enforcement," 2.

enterprise's normal process. [45] This definition encompasses most of the approaches to Red Teaming currently used within the U.S. intelligence community, defense, and homeland security.[46]

Examining the many definitions and their origins helps to gain insight into the fundamentals of Red Teaming. At its essence, Red Teaming is about the culture of an organization.[47] An effective use of Red Teaming or Red Team fundamentals involves more than the establishing a Red Team—it involves a process by which the Red Team concepts are received, understood and considered throughout an organization.[48]

C. RED TEAM'S ROLE

There are also significant differences of opinion within the literature regarding the approach Red Teaming should take. One set of authors argues that Red Teaming should be unstructured and operate at the planning, cognitive level, providing contrary and independent opinions while working outside the organization's decision-making process.[49] Others view Red Teamer's true role as serving as actual surrogate adversaries or competitors of the enterprise.[50] Still others within the Department of Army literature view the Red Teaming process as one of critical thought, aiding decision makers through a structured iterative process.[51] Within the homeland security literature, the approach to Red Teaming is viewed as a set of individuals who are experts—"bad actors" who innately understand how to undermine systems and specific types of targets to be

[45] Shelley Kirkpatrick, Shelly Asher, and Catherine Bott, "Staying One Step Ahead: Advancing Red Teaming Methodologies through Innovation" (Arlington, VA: Homeland Security Institute, 2005), 2. (FOUO).

[46] Ibid., 3.

[47] *The Role and Status of DoD Red Teaming Activities*, 1.

[48] Ibid., 3.

[49] Gregory Fontenot, "Seeing Red: Creating a Red-Team Capability for the Blue Force," *Military Review* 85, no. 5 (September 2005).

[50] Richard Craft, "A Concept for the Use of Red Teams in Homeland Defense" *Sandia National Laboratories* (September. 26, 2002).

[51] Malone and Schaupp, "The Red Team, Forging a Well-Conceived Contingency Plan," 23.

attacked.[52] Red Teaming can be an interactive process conducted during crisis action planning to assess planning decisions, assumptions, processes and products from the perspective of friendly partners, the enemy and others.[53] An effective Red Team can serve the enterprise as an independent resource for the decision maker by providing an independent review of the agency's products and reasoning. Even the most talented group of planners and critical thinkers cannot identify their own oversights, and sometimes are unable to see the overall big picture.[54]

At the strategic level an effective Red Team can assist by pinpointing key decision points for the leader, identify planning shortfalls, highlight differences between plans and doctrine, while also helping to identify unintended consequences, second- and third-order effects.[55] Red teaming can assist the decision maker and planners by contributing to a greater understanding of the overall security environment, and how adversaries might oppose and attempt to defeat U.S. security efforts.[56] Red Teaming in general offers a hedge against surprise and challenges complacency, as well as exposing how well an agency understands its own plans and procedures.[57] Each of these approaches and methodologies, although divergent in their perspectives are similar in their ultimate objectives and contributions to the Red Team context.[58]

There has also been a disparity on the issue of where to focus Red Teaming efforts, in terms of whether the focus should be entirely on role-playing adversaries, or if true emphasis is on challenging aspects, plans, programs etc.

---

[52] B. Tuchman, *The Guns of August* (New York, NY: Macmillan Publishing Co., Inc., 1962), 73.

[53] Malone and Schaupp, "The Red Team, Forging a Well-Conceived Contingency Plan," 23.

[54] Ibid., 24.

[55] *Red Team Handbook*, version 4, 23.

[56] Sandoz, "Red Teaming: A Means to Military Transformation," 17.

[57] Meehan, "Red Teaming for Law Enforcement," 3.

[58] Kirkpatrick et al., "Staying One Step Ahead," 2.

of the enterprise that establishes the Red Team.[59] Shifting the focus from the enemy perspective to the originating organization's perspective places the Red Team more in the role of the devil's advocate, enabling the team to offer a critique of the organizations assumptions, strategies, plans, concepts, programs, projects and processes, and sometime offering alternatives to those efforts.[60]

D. RED TEAMING HISTORICAL USE

The second sub area of literature related to Red Teaming explores its development through history. Researchers seem to agree that the origins of Red Teaming stem from the nineteenth century when German military strategists developed the Kliegspiele (war game). Kriegspiele, which was a rules-based map simulation war game, provided the opportunity to train and test concepts and plans, while evaluating leadership.[61] Post WWI, Germany, England, France, and the United States all utilized war-gaming on various levels to improve and/or validate lessons from WWI and develop plans for future conflicts.[62]

One of the best-documented war games is the Strategy and Force Evaluation (SAFE) hosted by Rand Corporation in the 1960s, which yielded branch points that inspired seminars to examine the consequences of the strategies selected and those rejected.[63] In the true sense of war-gaming, during the Cuban Missile Crisis (1962), President Kennedy organized the Executive Committee of the National Security Council to advise him on the situation and potential U.S. responses to the unfolding crisis.[64] This move was a deliberate attempt to consider alternative courses of action as a counterbalance to the

---

[59] *The Role and Status of DoD Red Teaming Activities,* 2.

[60] Ibid., 4.

[61] Gary D. Brewer and Martin Shubik. *The war game: a critique of military problem solving* (Harvard University Press, Cambridge, MA, 1979), 23.

[62] Homeland Security Advisory Council, "Top Ten Challenges facing the Next Secretary of Homeland Security" (Washington, D.C., Government Printing Office, September 11, 2008), 12.

[63] Dietrich Dormer, *The Logic of Failure: Why Things Go Wrong and What We Can Do To Make Them Right* (New York: Metropolitan Books 1996), 169.

[64] *The Role and Status of DoD Red Teaming Activities*, 3.

strong military response being advocated by other advisors, primarily military chiefs. Although not always called Red Teaming, the literature agrees that throughout history, the military and government decision makers have employed Red Teaming fundamentals during times of stress and conflict to provide decision makers with a better understanding of how their actions and decisions will be perceived by the enemy, alternative analysis, and a challenge to their own organization's assumptions.

E. CATEGORIZING TYPES OF RED TEAMING

The third sub area of literature dealing with the issue of Red Teaming relates specifically to the way Red Teaming is executed. Here there is significant incongruity about how to conduct Red Teaming. These varying methods of implementing the Red Team concept contribute in part to the confusion of establishing a definition.[65] Army Red Teaming can focus on very technical issues and vulnerability analyses, focusing on capabilities instead of the probability the enemy will use those capabilities.[66]

Categorizing the broad spectrum of Red Teaming approaches can be done upon two broad dimensions: (1) passive or active, and (2) structured or unstructured.[67] Active Red Teaming is often used to physically test friendly tactics before using them in a live or hostile environment. Active Red Teaming is used to train operational staff to respond to adversarial actions, by serving as surrogate adversaries and competitors.[68] The purpose of active Red Teams is to sharpen skills, expose vulnerabilities that adversaries might exploit and, in general, increase understanding of potential actions and counter-actions of potential adversaries.[69]

---

[65] *The Role and Status of DoD Red Teaming Activities*, 4.

[66] Ibid., 5.

[67] Malone and Schaupp, "The Red Team: Forging a Well-Conceived Contingency Plan."

[68] Kirkpatrick et al., "Staying One Step Ahead," 4.

[69] *The Role and Status of DoD Red Teaming Activities*, 4.

Passive Red Teaming is used to provide alternative perspectives, challenge existing assumptions, and identify how the enemy may adapt to U.S. capabilities.[70] These categories are reflected within the numerous Red Teams throughout the U.S. government.[71] The purpose of passive Red Teaming is to aid the organization by providing critical analysis in order to anticipate problems and avoid surprise.[72]

The literature specifically addresses these methods of facilitating Red Teaming by analyzing the different approaches of existing Red Teams.[73] For example, the Navy's program, although originally created to identify potential vulnerabilities that might put the U.S. Navy at risk, now evaluates and assesses findings from the intelligence community.[74] Comparatively, the Air Force Red Team program provides assessment of concepts and technology in order to evaluate and recommend friendly system improvements.[75]

One essential product of Red Teaming is the study and research of what the opponent or the enemy is doing in order to understand, avert, or at least mitigate the possible harmful effects of what the adversary plans to do.[76] The U.S now faces emerging threats that are more modern and better equipped in knowledge, information, and technology. This includes new technology in armament, new kinds of warfare, weaponry, and other dynamics of battle, coupled with wider fields of destruction and violent international fighting. The threat is also non-traditional; they are not nation states, but instead the potential opponents are fanatics and are committed to the extreme sacrifice of going

---

[70] Kirkpatrick et al., "Staying One Step Ahead," 4.

[71] Malone and Schaupp, "The Red Team: Forging a Well-Conceived Contingency Plan."

[72] *The Role and Status of DoD Red Teaming Activities*, 4.

[73] Malone and Schaupp, "The Red Team: Forging a Well-Conceived Contingency Plan."

[74] Ibid.

[75] Ibid.,

[76] *The Role and Status of DoD Red Teaming Activities*, 2.

suicidal in order to achieve their objectives.[77] This new threat was exemplified in the case with the hijackers on September 11, 2001, and has continued to evolve through the attempted bombing of Flight 253.[78]

The policy of using Red Teaming as a mechanism for threat emulation or threat assessment fails to fully utilize the broader scope of Red Teaming, which includes the analytical side of Red Teaming. Historically, military organizations have used wargaming with adaptive simulated enemies to test war plans, as well as emerging concepts.[79] The U.S. military has been using Red Teams to test their planning for over thirty years.[80]

DHS uses its Critical Infrastructure Red Team in a traditional role of threat emulator, seeking to understand the enemy's perspective and anticipate the enemy's conduct in order to role-play bad actors in DHS exercises. The goal is to improve security systems and personnel responses to enemy actions. These Red Teams seek to identify vulnerabilities within these critical infrastructure security systems so that areas of weakness can be identified and strengthened, and vulnerabilities eliminated or mitigated.[81] DHS Red Teams focus on how an identified or created advisory could defeat security systems of a particular critical infrastructure target.[82] Often, this physical Red Teaming entails individuals portraying actual, realistic, adversary action and counteraction to security procedures during an exercise. The Red Team will act according to a selected group's motivations, capabilities, and intent, based upon known terrorist tactics, techniques, and procedures.[83]

---

[77] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.*

[78] U.S. Senate, Homeland Security and Governmental Affairs Committee, "*Intelligence Reform: The Lessons and Implications of the Christmas Day Attack,"* Dennis Blair, Testimony (January 20, 2010).

[79] Peter Andrews, Executive Technology Report, *IBM Advanced Business Institute* (2005).

[80] Ibid.

[81] Alt, Critical Infrastructure.

[82] Ibid.

[83] Ibid.

Another one of the DHS Red Team strategies is to employ Red Team techniques within the intelligence and warnings area.[84] Within the Department of Homeland Security, as well as the homeland security community, a void exists in the area of decision support Red Teaming capabilities and the broader application of Red Team fundamentals. This capability is designed to assist leaders in thinking about the enemy's potential responses to security initiatives.[85] The Homeland Security Advisory Council recently highlighted this deficiency to the incoming Secretary by suggesting that a mechanism must be developed to enhance a leader's ability to think like our adversaries, or to look at problems through different lenses and challenge institutional assumptions.[86]

The U.S. has a continuing need to better understand and anticipate the adaptive and complex nature of our adversaries in order to reduce our vulnerabilities and increase security. [87] For years, the U.S. military has recognized this need to anticipate what the enemies' actions will be, thus the development of kriegspiele and wargaming as an effort to "write history in advance."[88] The Red Teaming concept is an extension of that historical effort to increase security and defeat or mitigate the impact of the enemies' actions.[89] The need for more extensive and broader applications of Red Teaming is greater today, due to increased complexity and the adaptive nature of the security threat facing the U.S.[90]

---

[84] Meehan, "Red Teaming for Law Enforcement," 1.

[85] *The Role and Status of DoD Red Teaming Activities*, 15.

[86] Homeland Security Advisory Council, "Top Ten Challenges Facing the Next Secretary of Homeland Security," (Washington, D.C., Government Printing Office, September 11, 2008), 12.

[87] Kirkpatrick et al., "Staying One Step Ahead," 1.

[88] Richard Sinnreich, "Red Team Insights from Army Wargaming," *Defense Adaptive Red Team Working Paper #02-3* (September 2002), 15.

[89] Ibid., 15.

[90] Kirkpatrick et al., "Staying One Step Ahead," 44.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RED TEAM FUNDAMENTAL CONCEPTS

We can't solve problems
by using the same kind of thinking
we used when we created them.

—Albert Einstein

The Red Team fundamentals include critical thinking and analysis to challenge and provide alternatives.[91] Critical thinking forms the foundation of Red Teaming. Our thinking, planning, and actions are often tainted, biased, distorted, partial or uniformed by our experiences or some starting point we use to filter information.[92] Red Teams use critical thinking to analyze plans, operations, and concept developments for the head of the agency. Although the leader can do this alone, it is often virtually impossible for the leader or the staff to avoid the gravitational pull of the organization, to see and interpret facts a certain way, and to support the agency position.[93] This thesis will examine a thorough a case study of a security risk posed to homeland security. By analyzing the security risk through analysis of the Red Team, fundamental concepts determine whether doing so would have improved the decision-making process.

A. ANALYZING TO CHALLENGE

One of the most critical Red Team analytical concepts and skill sets utilized by trained Red Teams is to identify and challenge stated and implied assumptions made by their organization. Assumptions are information accepted as truth in the absence of facts, and they are utilized to continue planning and operations.[94] Assumptions come in various forms, both stated and implied, that are used by decision makers to reach a conclusion. Some assumptions are the

[91] *Red Team Handbook*, version 4, 11.

[92] Linda Elder and Paul Richard, *The Miniature Guide to Critical Thinking Concepts and Tools*. 2nd Ed. (Dillon Beach, CA: The Foundation for Critical Thinking, 2005), 1.

[93] Longbine, "Red Teaming: Past and Present," 61.

[94] Headquarters Department of the Army, *Field Manual 5-0*: *The Operations Process* (Washington D.C., March 2010), 2–8.

result of mirror imaging, cultural bias, arrogance, or a product of successful patterns. By first identifying and then challenging these assumptions, the Red Team is allowed to raise the decision maker's awareness of the assumptions, see how the assumptions may impact his decision—or skew his and his staff's understanding of the operating environment. A thorough review of the assumptions can help ensure the assessment does not rest on faulty logic or a false premise. One of the most difficult challenges a decision leader can face is identifying hidden assumptions; ideas held to be true, often at the unconscious level, are seldom examined, and almost never challenged.[95]

B. THE ROLE OF DEVIL'S ADVOCATE

Challenging the status quo is often referred to as playing the "devil's advocate." A devil's advocate must provide closer scrutiny to the assumptions or mind set by challenging the prevailing wisdom, or strongly held view, by building the best possible case for an alternative explanation. This practice was originated by the Catholic Church during the canonization of a saint. The Church would appoint a canon lawyer to argue against the canonization of the candidate.[96] During the process, the "devil's advocate" took a skeptical view to challenge the position of the petition in order to fully exercise the process of canonizing a candidate, to expose any weaknesses, and to ensure only worthy candidates were approved for sainthood. Devil's advocacy takes a formal statement of a proposed course of action and analyzes the underlying proposal for inconsistencies, inaccuracies, and irrelevancies. A critique is then prepared of the proposed action by building the best possible case for an alternative explanation, based on this examination. If the organization's proposal is found to be unsound, the devil's advocate should develop a reanalysis of proposal.[97] This

[95] Longbine, "Red Teaming: Past and Present," 14.

[96] Virgil Robinson, comment on "History of the Devil's Advocate," The Possibility Advocate Blog, comment posted September 2008.

[97] Charles Schwenk, "Devil's Advocacy in Managerial Decisions," *Journal of Management Studies* 21, no. 2 (April 1984) 153–168.

technique is best used to challenge a key assumption or consensus that the organization cannot afford to get wrong. By deliberately challenging the organization's own plans, programs and assumptions, Red Teaming can identify strengths, weaknesses, opportunities and threats that were not considered, or not given proper critical review. This action will assist the leader and the organization in militating against the comfort or complacency of accepted assumptions and beliefs, and ensure the decision will withstand close scrutiny.

C. ALTERNATIVE ANALYSIS

Alternative analysis is used as a decision-support tool in numerous agencies within DoD, to include logistics acquisition and Army Corps of Engineer problem solving. Alternative analysis is accomplished by providing the decision maker with a different picture of the operating environment, framing the problem differently, presenting different potential solutions, and highlighting the vulnerabilities of the adversary.[98] .On key issues, where there are competing views within an organization, then a Team A/Team B analysis is one technique that can help decision makers understand the merits of both opposing views and facilitate an independent decision based upon the merits. This decision-support tool is utilized to provide the decision maker with greater understanding of the situation, problem, and overall operating environment. Alternative analysis is used to improve intelligence process and estimates. The Report to the President of the United States (2005) states:

> The widely recognized need for alternative analysis drives many to propose organizational solutions, such as "red team" and other formal mechanisms. Indeed, the Intelligence Reform and Terrorism Prevention Act mandates the establishment of such mechanisms to ensure that analysts conduct alternative analysis. Any such organs, the creation of which we encourage, must do more than just alternative analysis, though. The Community should institute formal system for competitive — and even explicitly contrarian —

[98] Longbine, "Red Teaming: Past and Present," 11.

> analysis. Such groups must be licensed to be troublesome. Further, they must take contrarian positions, not just ones that take a harder line.[99]

Some techniques used to generate alternative analysis involve analysis of competing hypotheses and Team A/Team B exercises, among others. The value of spending time and resources to conduct alternative analysis is found in the benefits to the organization and decision maker, through filling gaps in understanding, identifying vulnerabilities and opportunities, avoiding groupthink, mirror imaging, cultural missteps and organizational tunnel vision. Red Teaming is an organizational solution to ensure that alternative, even contrarian, positions receive adequate effort and attention by decision makers.[100] Decision makers and organizations that engage in alternative analysis improve their decision making, identify more effective action, and develop a more holistic understanding of the possible outcomes related to decisions. [101]

D. CONSIDERING ALTERNATIVE PERSPECTIVES

Alternative perspectives are designed as the antidote to the problem of groupthink and its negative impact on decision outcomes [102] Groupthink is defined as, "a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when members striving for unanimity override their motivation to realistically appraise alternative courses of action."[103] This problem can occur when a strong leader influences the group's analysis, or through group pressures to get the job done or slant their analysis a certain way. Bias and other behaviors can reduce the quality of analysis and ultimately the decision. A by-product of groupthink can appear when groups apply their

---

[99] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, "Report to the President of the United States" (March 31, 2005). 170.

[100] Ibid., 170.

[101] *The Role and Status of DoD Red Teaming Activities*.

[102] Phillip Johnson, "Effects of Groupthink on Tactical Decision-Making" (Monograph, School of Advanced Military Studies, Fort Leavenworth, Kansas, 2008).

[103] Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd rev. ed. (Boston: Houghton Mifflin, 1983), 9.

attitudes, capabilities beliefs, and cultural values to another. By anticipating potential cultural perceptions of partners and adversaries, the decision maker can anticipate second- and third-order effects of actions and decisions in a multi-cultural environment, and anticipate implications to other actions at the strategic or tactical level.

Surrogate Adversary/Role Play is one technique used to generate alternative perspectives. Trying to understand how a foreign leader or decision-making group may behave is a challenge. At the tactical level, Red Teams within DHS usually adopt this approach to attempt to role-play a certain threat group and attempt to defeat security systems and procedures.[104] The inherent risk involved in such an exercise is imputing or assigning the same motives, values, or understanding of an issue that the friendly organization or friendly leader holds. This problem is referred to as "mirror imaging." It typically occurs where analysts have spent years developing information and knowledge regarding a particular threat or enemy.[105] This base of accrued knowledge becomes a prison and stifles the analyst's creative thinking. By utilizing the technique of applying alternative perspectives to a problem, situation or course of action, the decision maker is better able to understand the enemies and U.S. security partners' beliefs, cultural constructs and values, which influence their decision making.[106]

Red Teaming fundamentals are tools that can be used by a group or an individual leader to develop greater situational awareness and make better decisions. An organization's planning and decision making can be significantly impacted by skilled, trained Red Teams. Unfortunately, educationally formed bias and a preference for certain analytical approaches to problem solving can make an organization's planning and decision making sub-optimal.[107] A common

---

[104] *The Role and Status of DoD Red Teaming Activities*.

[105] Longbine, "Red Teaming: Past and Present," 14.

[106] Ibid., 15.

[107] Elder and Richard, *The Miniature Guide to Critical Thinking Concepts and Tools*.

error made by leaders and groups in problem solving is the failure to account for the enemy's ability to adapt, and the constant changing picture of the operating environment.

The security environment facing the U.S. is constantly adapting and changing to counter U.S. security efforts. DHS leadership already uses Red Teams in an effort to identify how security threats are adapting to our technological advantages, but expansion of their usage, and usage of Red Team fundamental concepts, is an important area for further research.

IV. RESEARCH DESIGN

Leaders within the Department of Homeland Security, and those contributing to the security of our country, seek to make good decisions that will continue to ensure the safety and security of our country. To do so, they are often required to make and execute effective decisions faster than the enemy or threat can do the same. Unfortunately, the security-operating environment facing the United States continues to become more complex and often leads us to bad thought habits, which set failure in motion from the beginning.[108]

In this chapter, the researcher familiarizes the reader with the case organization and methodology, and discusses how the technique will be applied to the security situation involving the Christmas Day bomber and Flight 253 into Detroit. Case study methodology is routinely criticized because of its dependence on a single case, creating difficulty in reaching a generalized conclusion. The established goal of a researcher using case study methodology is to set parameters that could be applied in all research, thus even with a single case, one could draw realistic conclusions.[109] It can be increasingly difficult to analyze what was known prior to an incident, versus what is known after an incident occurs and a thorough investigation is completed.

Case studies provide a holistic understanding of the problem set. In a case study involving Flight 253 and the attempted bombing by Umar Farouk Abdulmutallab, an agent of Al Qaeda, the problem set is not about a single screening checkpoint failing. Instead, it asks why the layers of security implemented by TSA failed to stop this terrorist.

By identifying and challenging assumptions inherent within TSA's security system, analyzing the problem using an alternative, model and looking at the problem from different perspectives, could the system have been made more

[108] Dormer, *The Logic of Failure,"* 7.

[109] Winston Tellis, "Introduction to Case Study." *The Qualitative Report* 3, no. 2 (July 1997).

secure? Through the examination of these issues, this research hopes to address the overall issue of whether broader utilization of decision support Red Teaming will effectively assist DHS and its partners in making better decision to help make our country safer.

The goal of this research is to determine if more effective, broader utilization of decision support Red Teams and the fundamental concepts of Red Teaming can positively affect decision making within DHS. This research deals with the nature of the problem faced by the Department Homeland Security through the Transportation Security Administration of securing the some 450 airport terminals across the U.S. Currently, active physical Red Teams are developing across the homeland security horizon and the Border Patrol is establishing Red Teams.[110] Other agencies within DHS and partners with DHS are becoming increasingly interested in developing active Red Teams.[111] These teams are focused upon threat emulation and how to defeat existing security systems. Although this is valuable, by not also applying Red Team fundamentals —of challenging assumptions of the organization, alternative analysis in concept, planning and operational design, and alternative perspectives from friendly agencies and partners' points of view—DHS is missing an opportunity to create a learning organization from these various perspectives.

This research uses a selected case study, combined with evidence and analysis from historical examples, to determine if decision makers can benefit from Red Teams and Red Team fundamental concepts. The challenges posed to decision making within DHS, and symptoms of defective decision making, may provide evidence to support conclusions about Red Team utilization in the case study.

This case study analysis will help homeland security leaders become more familiar with the fundamentals of Red Teaming so that they can incorporate

[110] Foy Watson (COL, instructor, UFMCS) discussion during conference January 27, 2010.

[111] Observations from attending DHS Second Red Teaming Conference, March 2009.

them and challenge their staffs to utilize these fundamental Red Teaming concepts in the development of the organization's concepts, plans, and strategic initiatives.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDY AND EVALUATION

The Department of Homeland Security protects the United States transportation industry through its subordinate agency the Transportation Security Administration (TSA).[112] Created just two months after the 9/11 attacks, TSA has become a fixture of the airline transportation environment. TSA's stated mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce.[113] TSA's role in homeland security is to imagine, assess, and mitigate all threats in all modes of transportation.[114] It is first essential that we have an overview of the security systems that was designed to, and is acting to, keep terrorists from entering the United States. Transportation security begins at the origin of where transportation assets begin their journey to America's shores. Protecting America from future terrorist attacks cannot be dissected as an isolated issue. Denial of access to terrorists must also be considered in the overall threat to the issue of boarder security, involving facets of immigration enforcement, drug trafficking, and other illegal entries. The holes in our security that allow entry through our ports of entry, which would allow drug smugglers, illegal immigrants, and others to enter, would also allow a terrorist to gain entry to the U.S. Among the thousands of visitors, immigrants, and students who come to America every year, which one—admitted on a temporary visa, passport or other document who overstays that visa, or in fact never shows up for school—will be the next terrorist to kill Americans?

For purposes of this case study, we will focus on only one aspect of the overall TSA responsibilities, which is commercial airline security. Airline security refers to procedures as well as infrastructure designed to avoid security problems

---

[112] U.S. Government Accounting Office, Report to the Chairman, Committee on Homeland Security, House of Representatives: *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests* (Washington D.C. Government Printing Office, August 2008) GAO-08-958, 42.

[113] Transportation Security Administration, "Transportation Security Administration Mission Statement."

[114] *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program.*

aboard aircraft.[115] The perception amongst the media and most Americans is that security for air travel is entirely based in airports. Even after this most recent attempt by the Christmas Day bomber, the media focus is still on checkpoint security.[116] TSA continues to set the conditions for the perception that security of the airplane is set at the checkpoints. The checkpoints are there to make sure that terrorists cannot bring anything aboard the plane that would enable them to take it over or destroy it.[117] These are called "prohibited items" and cannot be brought to a checkpoint, into the secure area of an airport, or aboard an aircraft.[118]

The airport checkpoint, however, is just one layer of a multi-layer security approach used by TSA to ensure the security of the traveling public and the nation's transportation system.[119] Because of their visibility to the public, TSA is most associated with the airport checkpoints.[120] Other layers of security used by TSA include intelligence gathering and analysis, checking passenger manifests against watch lists, random canine team searches at airports, federal air marshals, federal flight deck officers, and more security measures—both visible and invisible to the public.[121]

---

[115] United States General Accounting Office *Aviation Security: Efforts to Measure Effectiveness and Address Challenges, Testimony before the Committee on Commerce, Science and Transportation, U.S. Senate, Statement of Cathleen A. Berrick, Director Homeland Security and Justice Issues,* Washington D.C. Government Printing Office, November 5, 2003 (GAO-04-232T), 2.

[116] Scott Mayerwitz, "What's Different With Airline Security Today A Look at How Air Travel Has Changed and What You Now Need to Do at the Airport."

[117] United States Government Accountability Office, *Report to Congressional Requesters: Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges*, Washington D.C. Government Printing Office, October 2009, (GAO-10-128) 1.

[118] Transportation Security Administration, "TSA: Travel Assistant."

[119] United States Government Accountability Office, *Report to Congressional Requesters*, 20.

[120] CBS News, 60 Minutes, "TSA Screening Is Security Theater."

[121] United States Government Accountability Office, *Report to Congressional Requesters*, 23.

A terrorist faced with multiple security layers is facing a stronger, more formidable system, and is more likely to be deterred or fail during the attempted attack.[122]

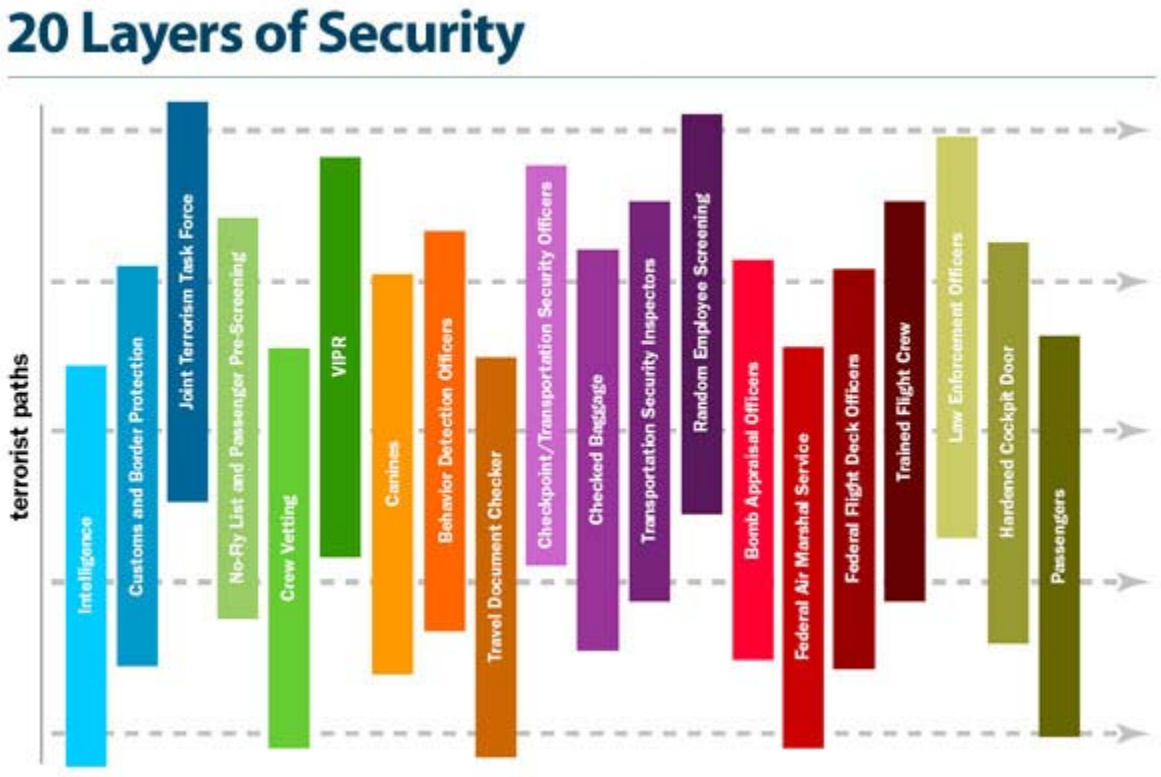

Figure 2. TSA Layers of Security

A. SECURITY LAYERS IN PLACE TODAY

Visible Intermodal Prevention and Response (VIPR), Travel Document Checker, Behavior Detection Officers (BDO), Secure Flight (software utilized to cross check traveler watch list), Federal Air Marshals (FAMs), Federal Flight Deck Officer (FFDO), Airline and support company Employee Screening and Checkpoint Screening Technology.[123]

[122] Transportation Security Agency, "TSA: Layers of security, what we do."

[123] Ibid.

The security systems TSA has arrayed, against a single or group of terrorists today to prevent their boarding and blowing up an airplane, appear to be overwhelming. This layered system of defenses is a monument to the hardworking men and women of TSA who go to work every day, and try to prevent another 9/11 style attack. Nevertheless, have they succeeded in making air travel safer? The only measurement of effectiveness that seems relevant is that, so far, no terrorist or group has succeeded in using a commercial aircraft as a weapon. TSA struggles with determining if its security initiatives are effective.[124] While it is true that no other terrorist attempts have succeeded, their success seems to be predicated on luck rather than actual effectiveness of TSA security efforts. When a terrorist event does not happen, is it because our security worked? Or were the terrorist merely unlucky? So far, we know TSA has succeeded in intercepting seven million prohibited items at airport checkpoints. If you break down those seven million items, only six hundred were firearms, which equates to .008 percent of items intercepted. Nearly 100 percent of what TSA succeeded in keeping off the airplanes consisted of items such as tweezers, breath fresheners, and lighters.[125]

These checkpoints at the 400 airports across the U.S. represent to most Americans TSA's security efforts.[126] TSA continues to enhance its security efforts at these checkpoints through investment of millions of taxpayer dollars in new technology, aimed at defeating prohibited items from making it on to commercial aircraft, yet gaps in security remain, and prohibited items still get through.[127] Despite TSA's attempts to build a robust, impregnable fixed-security

---

[124] United States General Accounting Office. *Aviation Security: Efforts to Measure Effectiveness and Address Challenges,* 20.

[125] Veronica Rugy, "TSA Disaster, Leave it to the government," *National Review Online*, (May 5, 2005).

[126] U.S. Senate, Committee on Commerce, Science and Transportation, *Implementing Recommendations of the 9/11 Commission Act of 2007,* October 16, 2007. Washington D.C., Government Printing Office, 2007.

[127] Homeland Security News Wire, "Billions spent on airport security, but major security gaps remain."

checkpoint and airport, no security is impenetrable.[128] Have we merely built a modern-age equivalent to the Maginot line? The Maginot line refers to a series of fortifications built along the French and German border, by France, as an impregnable defensive line through which no invaders army could pass. This method of defense, building fortress-type perimeters, dominated the French security mindset for years.[129] The French were so convinced that this static defensive line would protect them, they made basic assumptions that the heavily forested flanks of the Maginot line could not be effectively breached by tank units. This assumption ultimately proved false when the German Army outflanked the Maginot defensive line, leading to the ultimate defeat of France.[130]

TSA continues to focus on improving its security effectiveness of its airport checkpoints by investing in improved screening technology.[131] Yet, individuals, not just trained terrorists, continue to find ways to bypass, defeat, and outflank these security efforts. Are we building a technological Maginot line in our 400 airport checkpoints? Has the focus on identifying and stopping prohibited items caused a shift in America's airline security focus from catching and stopping *terrorist*, to stopping *things*?

Stopping terrorist attacks on the U.S. is the primary focus of several government agencies, and is a job that takes more than one agency's efforts to be successful at establishing and maintaining internal security.[132] One of the continuing hurdles faced by TSA and DHS is the institutional barriers created by bureaucracy. The silo effect of distinct cultures, budgets, and narrowly focused career ascendency compels government agencies toward self-protectiveness,

---

[128] U.S. Senate, Committee on Commerce, Science and Transportation, *Implementing Recommendations of the 9/11 Commission Act of 2007,* 3.

[129] Bryan Dickerson, "The U.S. Army vs. The Maginot Line," *Military History Online* (November 9, 2006).

[130] Ibid.

[131] Homeland Security News Wire, "Billions spent on airport security, but major security gaps remain."

[132] Arvind Gupta," Learning from the American Experience in Counter Terrorism," *IDSA Comment* (Institute for Defense Studies and Analysis, January 30, 2009).

insularity, and allegiance to their own agency-based advocacy and independence.[133] There are also deeply ingrained traditions of rivalry and palpable struggles for control, especially among organizations with similar or overlapping missions and scope of responsibility.[134] TSA, as part of the DHS counterterrorism effort, must be fully integrated into this effort, and unification of counterterrorist efforts must be empowered to occur between federal and state agencies.[135]

B. UMAR FAROUK ABDULMUTALLAB: THE CHRISTMAS DAY BOMBER

As a glaring example of failed airline security, Umar Farouk Abdulmutallab, a Nigerian citizen, is accused of trying to detonate an explosive device hidden on his body as the plane approached Detroit on a flight from Amsterdam on Christmas Day, 2009.[136] He was charged with trying to blow up a transcontinental airliner. The charges include attempted murder and trying to use a weapon of mass destruction to kill nearly 300 people.[137]

The federal criminal complaint filed against Mr. Abdulmutallab identified the explosive as pentaerythritol tetranitrate, or PETN. Umar had been placed on a UK watch list and barred from entering Britain earlier that year.[138] During his interview with FBI agents, Umar informed them that America could expect more attacks. He indicated there were more young men, just like him, in Yemen who would strike soon.[139] This was supported by a tape released four days before

---

[133] Leonard J. Marcus, Barry C. Dorn, and Joseph M. Henderson, "Meta-Leadership and National Emergency Preparedness, Strategies to Build Government Connectivity," *Working Papers, Center for Public Leadership,* (U.S. Center for Disease Control and Prevention, 2005) 43.

[134] Ibid., 42.

[135] Ibid.

[136] AP News Service, "Christmas Day Bomber Plead Not Guilty," *New York Post,* January 8, 2010, online edition.

[137] New York Times, "Umar Farouk Abdulmutallab," February 3, 2010, Times Topics, People, Online Edition.

[138] AFP, "Christmas Day bomber 'was on UK watch list,'" December 28, 2009, Online Edition.

[139] Brian Ross and Richard Esposito, "Abdulmutallab: More Like Me In Yemen," ABC News, December 28, 2009.

the attempted bombing of Northwest Flight 253, in which the leader of al Qaeda in Yemen boasted of what was planned for Americans:, "We are carrying a bomb to hit the enemies of God."[140] Umar had applied through the Department of State for a regular multiple-entry tourist visa, valid until June 12, 2010.[141]

C. AMERICA'S PERCEPTION OF TERRORISTS FUELED BY HOLLYWOOD

Today's media culture has created a picture of the modern terrorist by attempting to portray the essence of contemporary jihadist violence.[142] The terrorist exists beyond constraining factors of history, beyond politics, beyond psychology—a person defined as irredeemably evil and irrational.[143] The Hollywood mindset—that terrorists are Muslim fanatics—dominates film and often Americans' perceptions.[144] Even the U.S. intelligence community fell victim to this flawed perception when it developed a template for the modern terrorist, known as MAAM, "military-aged Arab male."[145]Terrorists are consistently portrayed as characters who are desperate, poor, uneducated and have few prospects.[146] This new "terrorist personality"—faceless, sinister, innately violent—has appeared hundreds of times over in the recent cycle of Hollywood terrorist-action films that continue to reap enormous box-office revenues.[147]

Umar, the Christmas Day Bomber, was not like the Hollywood terrorists. At 23, Umar led a life of privilege as the son of a prominent Nigerian banker. He

---

[140] Ross and Esposito, "Abdulmutallab: More Like Me In Yemen."

[141] The Whitehouse, "Remarks from the President on strengthening intelligence and aviation security."

[142] Carl Boggs and Tom Pollard, "Hollywood and the spectacle of terrorism," *New Political Science* (October 2006).

[143] Ibid.

[144] Gregory D. Miller, "Teaching about Terrorism: Lessons Learned at SWOTT," *Political Science & Politics,* **42**, 2009, 773–779.

[145] Malcolm Nance, "How (Not) to Spot a Terrorist," *Foreign Policy* (April 10, 2008).

[146] Miller, "Teaching about Terrorism," 775.

[147] Boggs and Pollard, "Hollywood and the spectacle of terrorism."

attended boarding school, and was an engineering student attending one of the leading universities in London.[148] Former counterterrorism czar Richard Clarke stated,

> This is the kind of person who lives in Europe and the U.S. who's being radicalized increasingly. Terrorists are often sons of middle to upper class families and from well-educated families who are being radicalized at long distance over the internet.[149]

Umar's father was previously the economics minister of Nigeria and recently retired as the chairman of the First Bank of Nigeria; he holds the Commander of the Order of the Niger, as well as the Italian Order of Merit.[150]

D. RED FLAGS AND WARNINGS

Dr. Magnus Ranstorp of the Center for Asymmetric Threat Studies at the Swedish National Defense College said,

> On the one hand, it seems he's been on the terror watch list but not on the no-fly list. That doesn't square because the American Department for Homeland Security has pretty stringent data-mining capability. I don't understand how he had a valid visa if he was known on the terror watch list.[151]

Umar's Father, Dr. Mutallab, had informed the U.S. embassy of his son's activities because of his growing concern about the radicalization of his son's religious views.[152] He was also reported to have been "surprised" his son had been allowed to travel after he had reported him to the authorities.[153] It was reported that the U.S. authorities had known for at least two years that Umar could have terrorist ties. He was on a list that included people with known or

---

[148] BBC News, "Police search London flat in US plane attack inquiry" (December 26, 2009).

[149] Ibid.

[150] Andrew Johnson and Emily Dugan, "The inside story of the privileged student who embraced al-Qaida and tried to blow a transatlantic jet out of the sky – and the lessons for us all," *The Independent*, December 27, 2009, Online Edition.

[151] Ibid.

[152] Tom Davenport, "Why they didn't connect the dots," *The Harvard Business Review* Blogs. Comment posted January 8, 2010.

[153] Johnson and Dugan, "The inside story of the privileged student who embraced al-Qaida."

suspected contacts or ties to a terrorist or terrorist organization.[154] The list is maintained by the U.S. National Counterterrorism Center and includes about 550,000 names.[155]

Another incident that was foreshadowing of the December 25 bombing attempt occurred on November 13, 2009: A man tried to board a commercial airliner in Mogadishu, Somalia, carrying powdered chemicals, liquid and a syringe, which was originally believed to have been capable of causing an explosion.[156] The case bears similarities to the plot to blow up the Detroit-bound airliner. The Somali man, whose name has not yet been released, was arrested by African Union peacekeeping troops before the Daallo Airlines flight took off. It had been scheduled to travel from Mogadishu to the northern Somali city of Hargeisa, then to Djibouti and Dubai.[157]

In response to the information received from Umar's father and other information the intelligence community collected, the U.S. embassy in Abuja sent a message to all U.S. diplomatic missions and the Department of State in Washington D.C., where the information was shared with the National Counterterrorism Center's Terrorist Identities Datamart Environment (TIDE) database.[158] Despite this fact, the derogatory information associated with Umar Farouk Abdulmutallab did not get shared thought the Intelligence Community.[159] Umar was not placed on either the No Fly or Selectee list, nor was his tourist visa revoked.[160]

---

[154] Johnson and Dugan, "The inside story of the privileged student who embraced al-Qaida."

[155] Ibid.

[156] CNN, "Somali forces: Would-be flier was not carrying 'bomb-making materials,'" December 31, 2009.

[157] Ibid.

[158] *Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part I,* Dennis C. Blair Testimony January 20.

[159] Jake Taper, Comment on "Hoekstra on Underwear Bomber: 'We Missed Him at Every Step.'" The ABC News Blog, comment posted December 28, 2009.

[160] *Intelligence Reform: The Lessons and Implications of the Christmas Day Attack.*

Hiding explosives in underwear is a new terrorist tactic, but the overall strategy remains the same—bring terrorism to America.[161] In August, in a failed terrorist assassination attempt on the Saudi Prince Mohammed bin Nayef, a suicide bomber used a similar technique of implanting explosives in his body.[162] This creates new challenges for airport screeners around the world, since a part of the explosive could be hidden either inside the inner thigh or wrapped over that area with skins, making it extremely difficult to detect during a normal airport screening search.[163] The ebb and flow between terrorist and defender continues to evolve, with each adapting and countering the other's move in a multi-turn game until one destroys the other.[164] Our defensive strategy in homeland security must be adaptive to the changing threats of modern terrorism.[165] A change in technology may defeat the terrorist threat posed today, but it will ultimately be defeated when the threat adapts.[166] Viewing this relationship between defender and terrorist as a coevolutionary dynamic relationship, provides the policy maker in homeland security with the opportunity to apply Red Team fundamentals to the problem, and opens the door to different solutions.[167]

There was so much information and intelligence available to our government indicating Al Qaeda and Umar's impending attack, yet our security and intelligence apparatus failed to identify them and take action until too late. Our government failed to connect, integrate, and understand the information we had. This indicates systemic failures and human error.[168] Our technological

---

[161] Bernard Debusmann, "The Underwear Bomber and the war of ideas," *Reuters*. December 31, 2009.

[162] Jamal Dajani, "Lost in Translation." *Link TV, Television without borders*. January 8, 2010.

[163] Ibid.

[164] Brian Jackson, "Technology Strategies for Homeland Security: Adaptation and Coevolution of Offense and Defense," *Homeland Security Affairs Journal* V, no. 1 (January 2009).

[165] Ibid.

[166] Ibid.

[167] Jackson, "Technology Strategies for Homeland Security: Adaptation and Coevolution of Offense and Defense."

[168] *The Lessons and Implications of the Christmas Day Attack,* Joseph Lieberman statement, (January 20, 2010).

advances were stymied by failure of accountability and overlapping responsibilities, which caused leads to not be followed to conclusion.[169] A tracking process between agencies, to determine agency actions and follow-up responsibilities regarding terrorist threats and warnings, is missing from our intelligence community.[170]

E. CHALLENGING THE ORGANIZATION'S THINKING

A fundamental concept of Red Teaming is to challenge the organization's thinking by questioning the assumptions made during the decision-making process and the conventional thought process of the group.[171] In this case study, despite TSA's 20 layers of security efforts, Umar Farouk Abdulmutallab did break through our defense and could have killed hundreds of innocent individuals if the explosive he hid in his clothing had worked.[172] TSA has undertaken numerous security initiatives to improve airport security since 9/11.[173] It also faces the challenge of managing almost 60,000 employees, 80 percent of whom work at airports to help screen passengers and their baggage.[174] Screening passengers and their bags is also where DHS spends the majority of its financial resources allocated for aviation security. In fiscal year 2004, DHS appropriated $3.7 billion for aviation security, $1.8 billion went to passenger screening and $1.3 billion for screening baggage.[175]

Although referred to a layered security system, aviation security is not provided through a truly systematic means, but rather through a collection of mostly unrelated measures that do not support one another or provide backup for

---

169 Whitehouse, "Summary of Whitehouse review of the December 25, 2009, attempted terrorist attack."

170 Ibid.

171 *The Role and Status of DoD Red Teaming Activities*, 11.

172 *The Lessons and Implications of the Christmas Day attack,* Joseph Lieberman statement.

173 *Efforts to Measure Effectiveness and Address Challenges, Statement of Cathleen A. Berrick,* 1.

174 U.S. Senate, Committee on Commerce, Science and Transportation, *Aviation Security,* 6.

175 Ibid., 25.

one another if one fails.[176] Unless the individual systems maintain a very high and sustained level of performance, an attacker could succeed by overcoming a single perimeter defense such as a security checkpoint, thus defeat the entire security system.[177]

Utilizing fundamental Red Team concepts, a decision support Red Team would analyze the implied assumptions in the TSA security system.[178] Strategic-level Red Teams analyze strategy and strategic decisions by challenging the organization's assumptions, by playing "devil's advocate," and challenging "conventional wisdom.[179] The current TSA security system focus is defensive in nature, establishing a final perimeter at the airport security checkpoint.[180] A Red Team might ask if we are building the equivalent of a modern-day Maginot line. What are the implied assumptions that aviation security is built upon? The current TSA security focus seems to be on keeping items off the plane, with the majority of their personnel involved in screening either passengers or baggage for prohibited items. Is that the proper focus for our aviation security system?

By shifting the paradigm from securing the transportation systems, to making the transportation systems secure by prohibiting forbidden items, to keeping prohibited persons off the plane, the focus of security shifts dramatically in how security resources are allocated.[181] A decision support Red Team would ask questions like: How do we shift our approach to aviation security from a defensive one to an offensive one? How do we identify those terrorist groups likely to try to smuggle explosives or other dangerous devices aboard

---

[176] Transportation Research Board, "Deterrence, Protection, and Preparation: The New Transportation Security Imperative" (Special Report 270, 2002, ISBN: 0-309-65604-4), 16.

[177] Ibid., 17.

[178] D. Cline, "Does The Theater Commander Really Know the Enemy? A Case for the Standing Theater 'RED CELL'" (Monograph, Naval War College, February 8, 2000), 20.

[179] Longbine, "Red Teaming: Past and Present," 8.

[180] Transportation Research Board, "Deterrence, Protection, and Preparation," 2.

[181] Kip Hawley, "Anticipating the Unexpected" (paper presented at IATA AVSEC World—Keynote Speech. Geneva, Switzerland, October 26, 2005.)

transportation systems? What types of devices are they likely to use? Where can you buy these explosives? How can we identify those who buy and supply the explosives to the terrorist?

El Al, the Israeli airline, is widely viewed as the most secure airline in the world, with the tightest security measures.[182] These security measures include at least one armed plainclothes sky marshal on each of its flights.[183] In the airport, a team of agents question passengers regarding the circumstances surrounding their flight: Why they are flying to a particular city, who they know at their destination, why they are going there, etc.[184] Michael Pangia, former FAA chief trial lawyer, said, "It is a matter of the job itself and how it is being approached."[185] If a similar tactic had been used, would Umar have been identified as a high-risk traveler?

Is our focus wrong? The U.S. aviation security system focuses on keeping weapons and bombs off airplanes, not necessarily on the people who board planes or a line of defense on the airplane.[186] Since 9/11, America's policy regarding airport and air travel security has been to federalize this important national task. James Carafano and Robert Poole, in their article: *Time to Rethink Airport Security*; argue that TSA is using the wrong security model. They argue that this move to federalize airport security is built on two assumptions: "A one size fits all passengers, in that they are all equally suspicious and should receive the same scrutiny, and the principal focus of airport security is to keep dangerous

---

[182] Miles O'Brien, "Model for air travel security may be El Al," CNN News (September 26, 2001.).

[183] Bob Simon, "The Safest Airline, A Secure Example Set By Israel's El Al." *60 Minutes, CBS News* (August 21, 2002).

[184] Christopher Walker, "Air security: rest of world needs to learn from El Al." *First Post* (January 21, 2010).

[185] Mike Fish "Part Three: Comparing U.S. to Europe, Outside the U.S., a different approach to air security. Tighter standards, better pay in Europe." *CNN News*. (November 16, 2001).

[186] Robert Poole and James Carafano, "Time to Rethink Airport Security" (Heritage Foundation, July 26, 2006).

objects (e.g., knives, guns, and bombs) off of airplanes."[187] These two assumptions lead to a myriad of actions on behalf of security personnel to counter the threat and create a perception that actually inhibits security. The government's approach to one size fits all security, by creating a standardized screening process, prevents TSA from identifying specific differences between airports and inhibits innovation and changes that could close this vulnerability gap, created by the one size fits all approach.[188] A decision support Red Team, focused on strategic assessment tools, would have questioned the security approach, because part of their job is to challenge the problem statement and assist in mitigating the reliance upon methods that have worked in the past, encouraging critical thinking by planners and decision makers.[189]

The economic operating environment for airline travel further complicates airport and air travel security. Passenger travel among the 100 largest U.S. airports can vary dramatically from year to year. Between 2003 and 2004, of the top 100 U.S. airports, 26 experienced an increase in passenger traffic of 11 percent to 50 percent, while three of these 100 airports experienced a decrease in passenger travel in a range of 5 percent to 35 percent. This unpredictable variability in passenger travel can cause airlines to move lines and change services from airport to airport, trying to find the most profitable route. In response, TSA can find itself with too few resources dedicated to an airport suddenly seeing a huge influx of passengers, while elsewhere, TSA screeners are waiting for passengers to appear.[190]

By reexamining and challenging the assumptions made in supporting the decision to federalize airport security, TSA will be forced to examine alternative solutions and approaches to securing air travel. Decision makers filter data regarding the operational environment through the mental model they have

[187] Poole and Carafano, "Time to Rethink Airport Security."

[188] Ibid.

[189] Longbine, "Red Teaming: Past and Present," 12.

[190] Poole and Carafano, "Time to Rethink Airport Security."

constructed to understand the situation.[191] This perception becomes a prison, constructed of old ideas and previous experience, which become barriers to considering all available possibilities.[192] To fully explore alternative security solutions, TSA may be required to expand its operational horizon beyond the airport or terminal and seek greater collaboration with other agencies also charged with the task of securing our country.[193] Finding the answers to the problem of securing the friendly skies by preventing terrorists from being able to buy a ticket in Amsterdam,[194] may go beyond the scope of TSA's mission, but not beyond the scope of DHS's mission. The unified effort to secure our airports has to be a collaborative effort, not just with other U.S. agencies, but other countries.[195] TSA, by reaching out to and collaborating with other government agencies while engaging and empowering other countries' security systems, can increase aviation security through offensive air travel security operations.[196] By challenging TSA's perception of its operational boundaries, a decision support Red Team could facilitate the removal of obstacles to providing a collaborative, integrated, aviation security system.

Currently, the TSA Red Team program is an offshoot of the original FAA Office of Civil Aviation Security program, created in response to the 1988 bombing of Pan Am Flight 103. Its primary mission is to conduct covert airport security penetration testing for identifying both localized and systemic vulnerabilities.[197] Although the TSA Red Team is providing a valuable function in

---

[191] Longbine, "Red Teaming: Past and Present," 12.

[192] Dormer, *The Logic of Failure*, 169.

[193] Transportation Research Board, "Deterrence, Protection, and Preparation: The New Transportation Security Imperative" (Special Report 270, 2002, ISBN: 0-309-65604-4), 11.

[194] Department of Homeland Security, *One Team, One Mission, Securing Our Homeland, U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008–2013* (Washington D.C. Government Printing Office, March 20, 2008), 3.

[195] Department of Homeland Security, "Secretary Napolitano to Discuss Ways to Bolster Global Aviation Security with International Partners in Mexico."

[196] Ibid.

[197] Catherine Rampell, "Ex-employee says FAA warned before 9/11." *USA TODAY*, November 24, 2006, Online edition.

testing airport security systems by broadening its mission or expanding the use of Red Team fundamental concepts,[198] the Red Team would be in a position to challenge the assumptions made in developing new security initiatives. Involving a Red Team in the concept development of new security approaches and technologies would help TSA and DHS meet the overall intent of the Homeland Security Authorization Act, by strengthening preemptive capabilities.[199]

F. ALTERNATIVE ANALYSIS

Alternative analysis can assist decision makers in identifying friendly and adversary vulnerabilities, accounting for the enemy's adaptive capability, and setting the problem.[200] Bruce Schneier, an airport security expert, states, "We've always known you can strap explosive material to your body without a metal triggering device and get it on a plane. You need to stop terrorists before they get to the airport."[201] If the problem is framed as the need to stop a deadly device from getting on the plane, can we really ever truly be successful at solving that problem? Through alternative analysis, a strategic decision support Red Team can offer different perspectives on the environment, problem, potential solutions and vulnerabilities of the adversary and the TSA aviation security system.[202]

Congress, by passing the Aviation Transportation Security Act, created a massive organization, involving the new personnel demand related to hiring, training and managing, at the time, a 45,000-person screening force.[203] By comparison, most other European countries have opted to do less with more, by adopting performance contracting to utilize private security screeners in lieu of

---

[198] United States Government Accountability Office, Committee on Homeland Security, House of Representatives; *TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests* (Washington D.C., GPO. August 2008), GAO-08-958.

[199] 49 U.S.C. 114(d).

[200] Longbine, "Red Teaming: Past and Present," 12.

[201] Kelsey Ramos, Comment on "Do tightened airport security measures protect us or distract from the problem?" *The LA Times* Blog, comment posted December 28, 2009.

[202] Longbine, "Red Teaming: Past and Present," 11.

[203] Aviation and Transportation Security Act (ATSA) – Public Law 107-71.

the American approach of having its national government assume operation of the passenger-screening system.[204] Analyzing the problem of air travel security by fundamentally altering the problem set—from preventing dangerous objects from getting on the aircraft, to preventing dangerous persons from getting on the aircraft—will change the range of potential security solutions available to TSA.[205] By focusing on the challenge of keeping the greater threat of terrorists getting on the plane, or from even being able to buy a ticket, the needs and demands for information for air travel security would change.[206] Shifting to a risk-based approach for screening potential passengers would involve categorizing them based upon information known to the TSA security system.[207] Dividing potential passengers into three broadly defined categories based upon the quality and quantity of information known about the traveler would categorize them as:

- Passengers about whom a great deal of information is available, thus are a low security threat;
- Passengers who fly less frequently and are traditionally leisure travelers; and
- Passengers about whom nothing is known, or there is specific negative information known about them.[208]

The advantages of such a risk-based approach would allow TSA and DHS to focus resources on the greater risk and threat to the security of air travel and generate increased intelligence and information demands to develop traveler

[204] Robert Poole, "The Case for Risk-Based Aviation Security Policy," *World Customs Journal* 3, no 2 (2009), 4.

[205] Poole and Carafano, "Time to Rethink Airport Security."

[206] Adrian Moore, "TSA's Airport Security Is Always a Step Behind, How a risk-based approach would focus resources on terrorists trying to bring down planes" (Reason Foundation January 27, 2010).

[207] Ibid.

[208] Poole, "The Case for Risk-Based Aviation Security Policy."

data profiles and focus on riskier travelers,[209] versus expending huge amounts of resources to screen the average flying public.

The current one-size-fits-all approach to airport security creates a perception of security that does little to impact the overall security of air travel. Instead, by applying different security measures to different passengers and their bags, the resources would be focused towards the greatest perceived threat and not on the average flyer.[210] Why spend resources screening a passenger with a current federal security clearance or who has a biometric identity card? These passengers should be allowed to board with minimum screening assets utilized on them or their luggage. A small percentage of these travelers could be randomly selected for more intensive screening. This would create disruptive patterns of security to deter potential terrorist from attempting to enter as a member of this passenger group.[211] This new security system might require infrequent, leisure travelers to go through a screening process similar to today's passenger screening process, but with alternating prohibited items based upon the current threat.[212] In addition, a percentage of this group could be identified for more thorough screening and interrogation as needed or supported by information collected.[213]

Finally, those travelers about whom little is known, would be thoroughly screened, both their persons and their checked and carry-on bags. Everyone in this group would receive a more rigorous screening, using the latest technology and techniques available, to determine if they are merely innocent travelers or in fact terrorists.[214] The concept of a risk-based passenger screening is not new. Identifying low-risk travelers in order to expedite their processing through airports

---

[209] Poole, "The Case for Risk-Based Aviation Security Policy."

[210] Ibid.

[211] Poole, "Toward Risk-Based Aviation Security Policy."

[212] Ibid.

[213] Ibid.

[214] Poole and Carafano, "Time to Rethink Airport Security."

was first recommended by aviation industry experts Michael Levine and Richard Golaszewski.[215] A proposed benefit of such a system was identified by Carnegie Mellon researchers, who suggested the time for processing passengers could be cut in half for frequent travelers, about whom a great deal of information is available. Such a system would stop wasting resources on low-risk passengers and would focus security on the security threat in proportion to the risk posed, thus putting the greatest resources against the greatest risk.[216]

The Red Team fundamental technique of alternative analysis used by a strategic decision support Red Team would re-examine the problem set facing air travel security operations. Instead of focusing on preventing dangerous items from getting on the aircraft, would the security system be more effective if the focus were on keeping terrorists off airplanes? The end result may be the same, but the shift in analysis would open decision makers and planners to different challenges and vulnerabilities before the enemy does.[217] Re-defining the problem of aviation security from prohibited items to prohibited persons is a critical step for decision makers, and the place where errors tend to occur.[218] A Red Team, by providing the decision maker with an independent resource for critically examining a problem, could dissect the symptoms of the problem from the true underlying "root problem," because alternative analysis examines the problems set from different understandings of the problem boundaries.[219] By analyzing the problem from different approaches, a TSA strategic Red Team can assist decision makers to better understand and work more effectively to solve

---

[215] Poole and Carafano, "Time to Rethink Airport Security."

[216] Catharine Foster, David Hamond, Mike Kaufman, Timothy Lo, Don Ojoko-Adams , Matthew Ragan and Jordan Schreck, "Short-Wait Integrated Flight Travel (SWIFT) System Applying Policy Changes, Technological Innovations, and Process Enhancements to Improve Airport Security and Efficiency" (PHD Diss., Carnegie Mellon University, May 7, 2003).

[217] *The Role and Status of DoD Red Teaming Activities*, Cover Memorandum.

[218] Headquarters Department of the Army, *Field Manual 5-0*: *Army Planning and Orders Production* (Washington D.C.,GPO. January 2005) 2–6.

[219] Longbine, "Red Teaming: Past and Present," 13.

the true aviation security problem.[220] TSA, acting alone, cannot solve this bigger problem of indentifying terrorists and keeping them off aircraft; it requires collaboration and information sharing within TSA and among other agencies.[221]. Through collaboration and synchronized efforts with local airport security, local police departments, other federal agencies, and transportation security agencies in other countries, TSA can develop joint concepts to help accomplish the overall mission, while also identifying vulnerabilities within our security systems.[222] This would allow TSA to better understand the capabilities of our adversaries and their adaptabilities, allowing TSA and their partners to anticipate situations of concern before they arise and adapt their security strategy to better position the U.S. for long-term success.[223]

G. ALTERNATIVE PERSPECTIVES

The third Red Team fundamental concept, examining a problem or issue through alternative perspectives, enable decision makers a better understanding of the operating environment by viewing an issue through the lens of other partners, agencies and adversaries, and other significant actors who can influence the environment.[224] Unfortunately, planning groups under pressure, trying to please their boss, can sometimes make faulty assumptions. This comes as a symptom of the problem of groupthink.[225] Under the Presidency of Harry Truman, his advisors shared the common opinion that Red China was a weak nation, whose main source of power in world affairs came from its affiliation with the Soviet Union, and thus its foreign policy was largely dominated by Russia.[226]

---

[220] Longbine, "Red Teaming: Past and Present," 13.

[221] Hawley, "Address to the Transportation and Terrorism Conference." (Speech presented at the Transportation and Terrorism Conference, July 30, 2008).

[222] *The Role and Status of DoD Red Teaming Activities*, 5.

[223] Longbine, "Red Teaming: Past and Present," 14.

[224] Ibid., 54.

[225] Phillip Johnson, "Effects of Groupthink on Tactical Decision-Making," (Monograph, School of Advanced Military Studies, Fort Leavenworth, Kansas, 2008). 7.

[226] Janis, "Victims of Groupthink," 247–278.

The advisors failed to take into account that this over-simplified perception might not apply to Red China's possible response to American troops in Korea. Therefore, they miscalculated the risk of provoking a full-scale military response to the U.S. attempt to use its military power to control China's ally and neighbor.[227]

In the case of Flight 253 and the events that led up to it, on December 23, law enforcement officials across the country, the FBI and the Homeland Security Department indicated that they had no specific credible intelligence indicating there were any plans from al-Qaida or any other terrorist groups to attack the U.S. during the holiday season.[228] The officials warn that al-Qaida and other terror groups "continue to seek innovative ways to conduct attacks and circumvent security procedures."[229] The U.S. counterterrorism system failed, because Umar Farouk Abdulmutallab should have been intercepted before he ever stepped on the plane.[230] In his testimony before Congress, the Director of National Intelligence admitted the need for applying Red Teaming fundamental concepts to the counterterrorism system by taking a penetrating look at the entire system.[231] In response to the December 25 incident, agencies across the federal government sprang into action to fix what the Abdulmutallab case indicated failed within the counterterrorism system.[232] Greater cooperation among DHS, the Department of State, the Department of Justice, the Intelligence Community, and others have been promised.[233] Nevertheless, will those promises be enough to

---

227 Janis, "Victims of Groupthink," 59.

228 John Amick and T. Rees Schiparo, "Security adviser: No smoking gun to stop attack." *The Washington Post.* January 3, 2010, Voices section, Online edition.

229 Hawley, "Address to the Transportation and Terrorism Conference."

230 U.S. Senate, House Committee on Homeland Security, "Flight 253: Learning Lessons from an Averted Tragedy," Statement for the Record of Michael E. Leiter. Director of the National Counterterrorism Center (Washington D.C., GPO. January 27, 2010).

231 "Flight 253: Learning Lessons from an Averted Tragedy."

232 Ibid.

233 Ibid.

create changes that will create a better counterterrorism system and bridge the gaps between international security and homeland security agencies?

TSA's mission is to secure the U.S. transportation system.[234] However, it never had the direct opportunity to interdict Abdulmutallab because, until he reached an American airport, TSA could only influence its partners in Amsterdam to screen him and deny him access through the secure flight program, which matches the watch list against the passenger manifest.[235] TSA also does not control or direct intelligence, but instead has influence over the intelligence collected through TSA's status as a consumer of intelligence.[236] In order to fix what went wrong in the Christmas Day bomber case, perhaps a greater effort should be made to consider intelligence through the lens of TSA and how quickly they need the information in order to be able to act upon it,

The enormity of the process TSA, and thus homeland security, must administer continues to filter and shape the environment. An estimated 1.2 million travelers from abroad seek to enter the U.S. by boat, air or land each day. Another 1.8 million travelers domestically board some 1,800 flights daily.[237] Although it is extremely difficult to look at a situation through someone else's lens or perception of the world, here it is obvious that the tremendous burden of screening every passenger, every bag, and treating each as an identical threat, creates vulnerabilities in the security system.[238] This security situation makes air travel a ripe target for future terrorist attacks.[239]

---

[234] Transportation Security Administration, "Transportation Security Administration Mission Statement."

[235] Department of Homeland Security Transportation Security Administration, 49 CFR Parts 1540, 1544, and 1560 Secure Flight Program; Final Rule, Federal Registry Vol. 73, No. 209 / October 28, 2008, 64034.

[236] Keith Kaufmann, Comment on "How Intelligence Drives Operations," The TSA Blog, comment posted March 4, 2008.

[237] "Flight 253: Learning Lessons from an Averted Tragedy."

[238] Poole and Carafano, "Time to Rethink Airport Security."

[239] Poole, "Toward Risk-Based Aviation Security Policy Discussion Paper No. 2008-23," *Joint Transportation Research Center* (Reason Foundation, November 2008), 17.

Until we understand the terrorists' perspective, grasping why blowing up an airplane—using it as a weapon—is attractive to them, we will continue to struggle with how to defeat these terrorist attempts.[240] If we can gain insight into their perspective of our security operations, then we can see the security environment through the eyes of a terrorist. Seeing the world through the eyes of the enemy is the trait of a good soldier.[241]

What if a terrorist announced his intended reaction to a proposed security system before TSA implemented it? What if the threat pointed out the flaws in the security plan and technology that he intended to exploit, and revealed several hidden weaknesses or indicators of his conduct? Surely, once the TSA and its partners optimized the strengths of its security plan and protected its vulnerabilities, the security system would be much more effective.[242] Red Teaming is the practice of viewing a problem from an adversary or competitor's perspective, thus enhancing the decision making through a broader understanding of the operational environment.[243] TSA and its partners can benefit from the implementation of a decision support Red Team and Red Team fundamentals, such as challenging assumptions, alternative analysis, and alternative perspectives to assist in their decision making and security concept design.

[240] Christopher Dickey, "A Thousand Points of Hate," *Newsweek*, January 2, 2010.

[241] Jeet Heer, "The Warrior Ethic: Respecting Your Enemy." *Sans Everything* (Wordpress, March 30, 2008).

[242] Malone and Schaupp, The "Red Team: Forging a Well-Conceived Contingency Plan."

[243] Mark C. Patterson and Sam Jin, Knowledge: Official Safety Magazine U.S. Army.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RED TEAMING'S FUTURE WITHIN DHS

To guess at the intention of the enemy; to divine his opinion of yourself; to hide from both your intentions and opinion; to mislead him by feigned maneuvers; to invoke ruses, as well as digested schemes, so as to fight under the best conditions—this is and always was the art of war.

—Napoleon

In the famous children's story, *The Emperor's New Clothes*, Hans Christian Anderson tells the tale of two tailors who hoodwink the emperor into believing they have made him a beautiful set of clothes, made from fabric so light and fine that it looks invisible to anyone who is too stupid and incompetent to appreciate its quality. Each of the emperor's trusted advisors, having been told of the claim by the tailors, reviewed the invisible, non-existent suit of clothes and proclaimed them extraordinary—for fear of being revealed as incompetent and losing their job. Finally, a child who had no important job proclaimed the truth: The emperor was naked and had no clothes.[244]

In modern times, the emperor is replaced by our president, with his arrays of trusted security advisors, all being influenced by experts spinning security systems and technological advances in exchange for payments of gold. Yet there is still the need for a young child to tell us the truth. Red Teams fulfill the function of Anderson's fairy tale. Red Teams are charged with telling the head of the agency that "what you invested in is not really providing you the security you hoped it would."

A. CONCLUSIONS

1. The terrorist threat facing the U.S. and its allies will attack our vulnerabilities, not our strengths. The terrorists are waging war asymmetrically

[244] Hans Anderson, *The Emperor's New Clothes*, Fairy Tales Told to Children, 1835.

and will attack our seams where vulnerabilities and gaps exist.[245] These adversaries are more likely to target and strike at vulnerable civilian targets or strike military targets in non-traditional ways, thus avoiding our military operational strength.[246] One of these systemic vulnerabilities is failure of imagination, which remains a factor within our homeland security institutions, five years after it was identified as an issue by the 9/11 commission.[247]

2. America's Homeland Security System is hampered by bureaucratic challenges. In order to effectively fight terrorism, the U.S. Government must dramatically re-orient itself.[248] By definition, imagination requires the entity to think about the way of doing business in a different manner.[249] Bureaucracies are not facilitators of creative original thought,[250] thus the culture of our government works against out of the box thinking which is necessary to fight terrorism. .

Despite our efforts the enemy keeps changing, adapting, and getting better at overcoming our defenses. Predicting future trends in terrorism has always been next to impossible. The actors involved have been few, their actions often erratic, and the behavior of small groups in society is no more predictable than that of very small particles in the physical world.[251] The Red Team concept is

---

[245] Robert Steele, TAKEDOWN: The Asymmetric Threat to the Nation. Joint Forces Quarterly (Winter 1998–99).

[246] United States General Accounting Office HOMELAND SECURITY A Risk Management Approach Can Guide Preparedness Efforts , October 31, 2001, Statement of Raymond J. Decker Director, Defense Capabilities and Management GAO-02-208T.

[247] Allison Graham, "The Ongoing Failure of Imagination." *Bulletin of the Atomic Scientists*, September/October 2006.

[248] Gail Russell Chaddock, "Failure of 'imagination' led to 9/11, The 9/11 final report assigns little blame, but cites many errors, and lays out bipartisan steps to avert future terror act," *Christian Science Monitor*.

[249] Douglas Jehl, "The New Magic Bullet: Bureaucratic Imagination," *The New York Times.* July 25, 2004.

[250] Nathan Luther, Bureaucracy: The Enemy Within. Proceedings.

[251] W. Laqueur, *No End to War: Terrorism in the Twenty-First Century*. New York, NY: Continuum International Publishing Group Inc., 2003.

however, uniquely capable of addressing the issue of terrorism, especially the threat that it poses to domestic security issues.[252]

3. Five Years after the 9/11 Commission, although tremendous changes have occurred, we still struggle with getting it right. America's need to redefine its homeland security approach into a flexible adaptive system, is a continuing problem as America's current and future threats are global and adaptive, blurring distinctions between crime, terrorism, and war.[253] Given the asymmetric nature of the threat, knowing what the United States is doing, "blue" is as critical as understanding "red," what our enemies are doing.[254] Department of Homeland Security was created by the President in order to create collaboration and cooperation between federal agencies.[255]

How then do we create a virus or antibodies within these critical homeland security institutions to protect, nurture, and develop an antidote for strategic surprise? Broader application of Red teams and implementation of their fundamental concepts, when supported by the leadership, create such antibodies within the organization.[256] Trained Red Teams applying creative thinking and their fundamentals, challenge the organizations assumptions, provide alternative analysis to the organizations plans and provide the decision maker alternative perspectives on the current operating environment.[257]

The case study in the previous chapter is presented to demonstrate the usefulness of applying Red Team fundamental concepts to current issues facing

---

[252] Culpepper, Effectiveness of Using Red Teams to Identify Maritime Security. Vulnerabilities to Terrorist Attack.

[253] Gregory F. Treverton, The Next Steps in Reshaping Intelligence, RAND Corporation: Santa Monica, CA.

[254] Ibid.

[255] Dara Kay Cohen, Mariano-Florentino Cuéllar, and Barry R. Weingast, "Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates."

[256] Susan Craig, "Reflections from a Red Team Leader," *Military Review,* March–April, 2007.

[257] Fishbein and Treverton, "Making Sense of Transnational Threats." The Sherman Kent Center for Intelligence Analysis. *Occasional Papers* 3, no. 1, October 2004, Sherman Kent Center.

Homeland Security decision makers. The analysis is rather simplistic, but applied by a trained Red Team, with time and resources; the Red Team's analysis can be insightful for decision makers to determine if they might "have got it wrong."[258]

The case study analysis identifies some recommendations that warrant further discussion and research regarding, potentially improving air travel security, the intent of this analysis is to demonstrate how greater application of Red Team fundamentals and broader application of Red Teams within homeland security would be beneficial to the decision making process. Currently DHS and several agencies within DHS have Red Teams, or are in the process of forming Red Teams to utilize primarily as threat emulators.[259] Using Red Teams in this manner is extremely useful to test the vulnerabilities of security systems and beneficial to accomplishing the overall DHS mission.[260] However, using Red Teams as threat emulators only utilizes a small portion of the potential Red Team capability that a trained Red Team provides through full-spectrum iterative operations and operating environment analysis from perspectives, which can help decision makers identify strategic vulnerabilities and develop mitigating strategies[261]. Broader usage of decision support Red Teams and Red Team fundamentals within DHS can assist decision makers in security system management, across the life cycle from concept through retirement.[262] Red Teams are particularly useful in identifying how the enemy will react to potential security improvements, strategy and policy changes.[263]

---

[258] Warren Fishbein and Tom Treverton, "Making Sense of Transnational Threats."

[259] Eileen Sullivan, CQ Homeland Security – Local Response. CQ Today. June 13, 2007.

[260] Ibid.

[261] Fontenot, Seeing Red, Creating a Red-Team Capability for the Blue Force, *Military Review,* September–October 2005.

[262] Red Teaming for Program Managers, Sandia National Laboratories.

[263] Malone and Schaupp, "The "Red Team" Forging a Well-Conceived Contingency Plan," *Aerospace Power Journal*, Summer 2002.

B. RECOMMENDATIONS

Education on the Red Team Fundamentals should be implemented as mandatory for all homeland security leaders. Homeland Security Leaders need to become more familiar with the basic precepts of Red Teaming so that they can incorporate them into their decision making process and challenge their staffs to utilize these concepts in the development of plans and strategic initiatives.

1. Ask Questions

At a minimum, homeland security leaders should be trained to begin asking the following four questions of projects that are presented to them:[264]

1. "What if….?" This question is useful in trying to anticipate what the enemy may do.

2. "What are the objectives of…?" Answering this question forces the staff to consider other perspectives, those of the enemy, of other partner nations, of other agencies working towards the same mission of homeland security.

3. "What are we missing…?" Answering this question helps identify seems gaps and vulnerabilities within your own agencies operations, plans, and conceptual designs. It could also identify disconnects between your agency and another that need to be filled in order to avoid exploitation.

4. "What is working and what isn't?"[265] This question helps create homeland security leaders in creating a learning organization, which provides a work culture that is open to creative thought, empowering employees to think critically and creatively, while giving them the ability to communicate ideas and

[264] UFMCS handbook version IV, FOUO.

[265] Ibid.

concepts, and the ability to cooperate with each other in the process of inquiry and action,[266] while avoid establishing patterns of operation that can then be identified and defeated by the enemy.[267]

These questions are simple, but the concepts behind them are not so simple. While asking the questions may help identify problems, solving them will take more effort and creativeness on behalf of the organization. Asking these questions of their staff will help homeland security leaders better understand the gaps and vulnerabilities within their organization's planning. This basic Red Teaming fundamental technique can be very beneficial to an organization, by offering a hedge against surprise and inexperience and a guard against complacency.[268] By asking these questions and using Red Teaming fundamental concepts, the leader begins to tests the fusion of policy, operations, and intelligence. Red Teaming can be used to imitate attackers, other agencies, even Murphy's Law, thus creating a closely synchronized planning staff, drive more complete analysis, and deliver a better plan.[269] Through analysis, a trained Red Team can identify deviations from doctrine, reveal overlooked opportunities, and determine how well an agency understands its own plans and procedures.[270]

Beyond leadership education, skilled and trained Red Teaming

> provides a means to build intellectual constructs that replicate how the enemy thinks [because the constructs] rest on a deep intellectual understanding of his culture, [the] ideological (or religious) framework through which he interprets the world…and his possible and potential strategic and operational moves.[271]

---

[266] Moya Mason, "What is a Learning Organization?"

[267] Headquarters Department of the Army Washington, DC, Field Manual No. 20–3 ,Chapter 3, 3–1, August 30, 1999.

[268] Malone and Schaupp, "The Red Team: Forging a Well-Conceived Contingency Plan."

[269] Ibid.

[270] Ibid.

[271] Murray Williamson, *Red Teaming: Its Contributions to Past Military Effectiveness* (McLean, VA: Hicks and Associates, September 2002), 58.

By carefully understanding and accurately imitating the enemy, an agency lessens the likelihood it will be caught by surprise and left unprepared. Effective use of Red Team fundamentals increases an organization's opportunities by challenging aspects of plans, programs, and assumptions. Through the eyes of the enemy, Red Teaming can assist organizations to prepare for the unexpected.[272] Homeland security leaders, by better understanding Red Teaming fundamentals, will know when to ask for alternative analysis and what to expect from alternative analysis.[273] Finally, knowing the enemy and viewing the security-operating environment from the enemy's perspective is an enabling skill set which will aid homeland security leaders in the understanding and anticipation of the adaptive and complex nature of the adversary.[274]

2. Implement Support Teams

DHS should implement decision support Red Teams as part of their force structure.

Although Red Teams are currently being used within DHS, Decision support Red Teams need to be utilized by key DHS leaders. Decision support Red Teams should be implemented and used by DHS agency heads and critical division within the organization. This will provide DHS leaders an independent capability for alternatively analyzing issues facing the organization, provide an alternative perspective regarding the agencies plans, concept designs and security programs. These perspectives may be for the perception of other U.S. government agency perspective, the perspective of our international partners and our potential enemies.

---

[272] *The Role and Status of DoD Red Teaming Activities*, 14.

[273] Ibid.

[274] Kirkpatrick et al., "Staying One Step Ahead: Advancing Red Teaming Methodologies through Innovation" (Arlington, VA: Homeland Security Institute, 2005), 1.

3. Implement Joint Enterprise

DHS should implement joint enterprise Red Teams between its own agencies and facilitate joint enterprise Red Teams between DHS and other security agencies, entities and partners.

In addition to internal DHS Red Teams, the leaders of homeland security should consider joint enterprise Red Teams who would be comprised of members from several U.S. agencies, i.e., Department of State, FBI, Border Security, TSA, National Counterterrorism Center, local and regional law enforcement agencies. Involving these various agencies provides a multidiscipline approaches to security and will help address multi-jurisdictional issues, while exploring opportunities for additional integrated security operations such as the current TSA VIPR program.[275] This joint enterprise Red Team could be charged with examining intelligence process within various agencies, information sharing and collaborative security efforts. An advantage to creating a joint enterprise Red Team would be to bring members from various agencies and security partners to provide various incites to security issues and barriers to information sharing. This concept of a joint enterprise Red Team could also be utilized with international partners, to assist in identifying cultural barriers within the U.S. governmental agencies and international government agencies that serve to inhibit the development of efficient effective collaborative security solution, while also identifying potential solutions to overcoming those barriers.

4. Implement Technology Development

DHS should implement Red Team integration into the Homeland Security technology approval process. Finally, Red Teams should be involved in the Homeland Security technology approval process.[276] Congress has instituted efforts to facilitate guidance and focused technology development in HLS. In

[275] Transportation Security Administration, VIPR Teams Enhance Security at Major Local Transportation Facilities, June 20, 2007.

[276] "U.S. Homeland Security (Government and Private) Market Outlook – 2007–2011," Homeland Security Research, January 2007.

2002, the U.S. Congress passed the SAFETY Act: (Support Anti-terrorism by Fostering Effective Technologies Act). Congress's intent was to create a technology clearing house to indentify and facilitate the development and deployment of anti-terrorism technology by creating systems of "risk management" and "litigation management." The systems are designed to provide liability protection in certain circumstances to DHS-approved "Qualified Anti-Terrorism Technologies" (QATTs). The law was designed to facilitate broader and deeper involvement of industry in the creation of needed technologies to assist in the protection of the homeland and defeat terrorist tactics and operations.

The current role of Red Teaming in technology development is varied, depending upon which federal agency is using the Red Team. Across the Department of Defense, Red Teams are tasked to provide assessments of concepts and technology, instead of their traditional roles as surrogate adversary.[277] When Red Teams become involved in technology development, their Red Team process involves red/blue interaction in order to evaluate and recommend blue system improvements. The Red Team provides a disciplined approach to guide decision making in technology development. The team also provides warnings regarding the vulnerability of fielded capabilities and gives insight into determining what sensitive information they are to protect. By looking at the technology from the enemy's perspective, often gapping vulnerabilities may be exposed.

The need for Red Teaming in technology development is illustrated by the fact terrorists regularly find ways to defeat or thwart our technological superiority. In trying to understand how terrorist groups overcome defensive technologies, the RAND Corporation determined that terrorists typically respond to defensive technologies by: altering operational practices, making technological changes or substitutes, avoiding the defensive technology, or attacking the defensive

[277] *The Role and Status of DoD Red Teaming Activities*, 11.

technology.[278] The enemy knows of our technological superiority and adapts basic tactics that often defeat our technology. One example comes from Afghanistan. The Taliban, cognizant of the fact the U.S. could listen to their telephone conversations over wireless phones, would traditionally communicate important information only face to face. For other communications, they developed code to shorten the communication time. They also injected an element of deception by communicating in a manner intended to deceive the listener as to their true intentions.

The Red Team Concept should be utilized and implemented by the DHS Science and Technology Directorate in the SAFETY Act implementation office. Currently, the regulatory approval cycle for technologies applying to DHS is 120 days from application to approval. During the 120-day regulatory cycle of the DHS approval cycle, a Red Team should assess the technology being presented. The Red Team assessment will look at the technology from the enemy's perspective.

This assessment will lead to improved design and implementation of the system throughout its life cycle. The Red Team can play the role of the Oppositional Force, providing constrained, reproducible, adversarial perspective to generate likely adversary observables to test detection and train blue force actions. Through experiments, the Red Team can explore technology's response to the stimulus of an adversary and determine the preferred response of the system, while also validating the system and identifying operational constraints.

[278] Brian Jackson et al., Breaching the Fortress Wall: Understanding Terrorist Efforts to overcome Defensive Technologies, RAND Corporations 2007.

BIBLIOGRAPHY

49 U.S.C. 114(d).

911 Commission Report, 2004.

Allison, Graham. "The Ongoing Failure of Imagination." *Bulletin of the Atomic Scientists*, September/October 2006. http://belfercenter.ksg.harvard.edu/publication/958/ongoing_failure_of_imagination.html (accessed March 17, 2010).

Alt, Richard, Critical Infrastructure Red Team, Brochure, Undated.

Amick, John, and T. Rees Schapiro. “Security adviser: No smoking gun to stop attack.” *The Washington Post*. http://voices.washingtonpost.com/44/2010/01/security-adviser-no-smoking-gu.html (accessed March 10, 2010).

Anderson, Hans. *The Emperor's New Clothes, Fairy Tales Told to Children, 1835*.

Andrews, Peter. Executive Technology Report, IBM Advanced Business Institute, http://www-935.ibm.com/services/us/imc/pdf/gt510-6190-red-teams.pdf (accessed March 31, 2010).

Associated Press. “Christmas Day Bomber Plead Not Guilty,” *New York Post,* http://www.nypost.com/p/news/national/christmas_day_bomber_to_be_arraigned_Ky5FfaM7t5a9VXOyLO8UIM (accessed March 11, 2010).

Aviation and Transportation Security Act (ATSA) – Public Law 107–71.

BBC News. “Police search London flat in US plane attack inquiry.” December 26, 2009. http://news.bbc.co.uk/2/hi/8430872.stm (accessed March 11, 2010).

Blair, Dennis C. Testimony before Senate Homeland Security and Governmental Affairs Committee, January 20, 2010, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=db07fd72-c631-42ea-a514-215127425e3a (accessed January 23, 2010).

Boggs, Carl, and Tom Pollard. “Hollywood and the spectacle of terrorism*,” New Political Science,* October 2006. http://www.ocnus.net/cgi-bin/exec/view.cgi?archive=103&num=26261 (accessed March 11, 2010).

Brewer, Gary D., and Martin Shubik. *The war game: a critique of military problem solving* (Harvard University Press, Cambridge, MA, 1979), 23.

Brown, Gerald, Mathew Carlyle, Javier Salmeron, and Kevin Wood. Defending Critical Infrastructure, Interfaces 36(6), 530–544, 2006 http://interfaces.journal.informs.org/cgi/content/abstract/36/6/530 (accessed March 31, 2010).

A Case for the Standing Theater "Red Cell" Naval War College, February 8, 2000.

CBS News, 60 Minutes, TSA Screening Is Security Theater, July 31, 2009, http://www.cbsnews.com/stories/2008/12/18/60minutes/main4675524.shtml?tag=contentMain;contentBody (accessed March 8, 2010).

Chaddock, Gail Russell. “Failure of 'imagination' led to 9/11, The 9/11 final report assigns little blame, but cites many errors, and lays out bipartisan steps to avert future terror acts.” *Christian Science Monitor*. http://www.csmonitor.com/2004/0723/p01s03-uspo.html/(page)/2 (accessed March 22, 2010).

“Christmas Day bomber 'as on UK watch list.' “AFP, December 28, 2009, http://www.google.com/hostednews/afp/article/ALeqM5juvSYNQxU1fSopnJOrkXac_wJ0uQ (accessed January 14, 2010).

Cline, Donald. Does the Theater Commander Really Know the Enemy? Naval War Coll Newport RI Joint Military Operations Dept, February 8, 2000.

CNN. Somali forces: Would-be flier was not carrying 'bomb-making materials.' December 31, 2009. http://www.cnn.com/2009/WORLD/africa/12/31/somalia.airline.arrests/index.html (accessed March 11, 2010).

Cohen, Dara Kay, Mariano-Florentino Cuéllar, and Barry R. Weingast. Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates. http://politicalscience.stanford.edu/faculty/documents/weingast-crisis%20bureaucracy.pdf (accessed March 22, 2010).

Commerce, Science and Transportation, U.S. Senate. Statement of Cathleen A. Berrick, Director Homeland Security and Justice Issues, GAO-04-232T, 2.

Craft, Richard. “A Concept for the Use of Red Teams in Homeland Defense” Sandia National Laboratories, September 26, 2002.

Craig, Susan. “Reflections from a Red Team Leader.” *Military Review,* March–April, 2007. http://www.au.af.mil/au/awc/awcgate/milreview/craig.pdf (accessed March 17, 2010).

Culpepper, Anna. Effectiveness of Using Red Teams to Identify Maritime Security. Vulnerabilities to Terrorist Attack, Naval Postgraduate School Monterey, California. Thesis

Dajani, Jamal. “Lost in Translation. Link TV, Television without borders.” January 8, 2010. http://www.linktv.org/mosaic/blog/keyword/prince_mohammed_bin_nayef (accessed March 11, 2010).

Davenport, Tom. “Why they didn’t connect the dots.” *Harvard Business Review* Blogs. January 8, 2010. http://blogs.hbr.org/davenport/2010/01/why_they_didnt_connect_the_dot.html (accessed March 11, 2010).

Debusmann, Bernard. The Underwear Bomber and the war of ideas. Reuters. December 31, 2009. http://blogs.reuters.com/great-debate/2009/12/31/the-underwear-bomber-and-the-war-of-ideas/ (accessed March 11, 2010).

Department of Defense, Defense Science Board, *Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities,* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September 2003).

Department of Homeland Security Transportation Security Administration, 49 CFR Parts 1540, 1544, and 1560 Secure Flight Program; Final Rule, Federal Registry Vol. 73, No. 209. October 28, 2008, 64034. http://www.tsa.gov/assets/pdf/secureflight_final_rule.pdf (accessed March 17, 2010).

Department of Homeland Security. One Team, One Mission, Securing Our Homeland U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008–2013 http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf (accessed March 31, 2010).

Dickerson, Bryan, “The U.S. Army vs. The Maginot Line,” November 9, 2006, http://www.militaryhistoryonline.com/wwii/articles/maginotline.aspx (accessed March 8, 2010).

Dickey, Christopher. “A Thousand Points of Hate, *Newsweek*.” January 2, 2010. http://www.newsweek.com/id/229078/page/1 (accessed March 17, 2010).

Dormer, Dietrich, *The Logic of Failure: Why Things Go Wrong and What We Can Do To Make Them Right*. New York: Metropolitan Books 1996, 169.

Elder, Linda, and Paul Richard, *The Miniature Guide to Critical Thinking Concepts and Tools.* 2nd Ed. (Dillon Beach, CA: The Foundation for Critical Thinking, 2005).

Field Manual 5-0, Section 2-6. Army Planning and Orders Production, Headquarters Department of the Army, January 2005.

Fish, Mike. Part Three: Comparing U.S. To Europe Outside the U.S., a different approach to air security, Tighter standards, better pay in Europe. CNN News. November 16, 2001. http://www.cnn.com/SPECIALS/2001/trade.center/flight.risk/stories/part3.mainbar.html. (accessed February 15, 2010).

Fishbein, Warren, and Gregory Treverton. "Making Sense of Transnational Threats." The Sherman Kent Center for Intelligence Analysis. *Occasional Papers* 3, no. 1, October 2004, https://www.cia.gov/library/kent-center-occasional-papers/vol3no1.htm (accessed March 17, 2010).

Fishman, J. "The Need for imaginations in International Affairs." *Israel Journal of Foreign Affairs III*, 2009, 3.

Fontenot, Gregory. "Seeing Red: Creating a Red-Team Capability for the Blue Force." *Military Review* 85, no. 5 (September 2005).

Foster, Catharine, David Hamond, Mike Kaufman, Timothy Lo, Don Ojoko-Adams, Mathew Ragan, Jordan Schreck, David Stopp, and Ryan Wilson. Short-Wait Integrated Flight Travel (SWIFT) System Applying Policy Changes, Technological Innovations, and Process Enhancements to Improve Airport Security and Efficiency. May 7, 2003. http://www.heinz.cmu.edu/research/135full.pdf (accessed March 16, 2010).

Gladwell, Malcolm. *Blink: The Power of Thinking Without Thinking*. Back Bay Books (2007).

Gold, T., and B. Hermann. *Defense Science Board task force on role and status of DoD red teaming activities*. Washington: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. 2003. http://www.acq.osd.mil/dsb/reports/redteam.pdf (accessed March 16, 2010).

Gordan, Michael, and Bernard Trainor. *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon Books, Random House Inc. 2006), 311.

Gupta, Arvind. Comment, Institute for Defense Studies and Analysis, January 30, 2009. http://www.idsa.in/idsastrategiccomments/LearningfromtheAmericanExperienceinCounterTerrorism_AGupta_300109 (accessed March 9, 2010).

Hawley, Kip. Anticipating the Unexpected. IATA AVSEC World. Keynote Speech. Geneva, Switzerland, October 26, 2005. http://www.tsa.gov/press/speeches/speech_1003.shtm (accessed March 15, 2010).

———. Address to the Transportation and Terrorism Conference. July 30, 2008. http://www.tsa.gov/press/speeches/073008_hawley_fbi.shtm (accessed March 16, 2010).

———. U.S. Department of Homeland Security; Testimony before the U.S. Senate Committee on Commerce, Science and Transportation, October 16, 2007. http://www.tsa.dhs.gov/assets/pdf/10-16-07_Testimony_SCST.pdf (accessed March 8, 2010).

Headquarters Department of the Army Washington, DC, Field Manual No. 20-3, Chapter 3, 3–1, August 30, 1999. http://www.globalsecurity.org/military/library/policy/army/fm/20-3/ch3.htm (accessed March 22, 2010).

Heer, Jeet. “The Warrior Ethic: Respecting Your Enemy.” *Sans Everything,* March 30, 2008. http://sanseverything.wordpress.com/2008/03/30/the-warrior-ethic-respecting-your-enemy/ (accessed March 17, 2010).

Homeland Security News Wire, “Billions spent on airport security, but major security gaps remain,” February 8, 2008. http://homelandsecuritynewswire.com/billions-spent-airport-security-major-security-gaps-remain?page=0,0 (accessed March 8, 2010).

Hosmer, Stephen T. “Why the Iraqi resistance to the coalition invasion was so weak.” http://www.rand.org/pubs/monographs/2007/RAND_MG544.pdf (accessed February 2, 2010).

Leiter, Michael E. Statement for the Record. Director of the National Counterterrorism Center House Committee on Homeland Security, “Flight 253: Learning Lessons from an Averted Tragedy.” January 27, 2010. http://www.dni.gov/testimonies/20100127_testimony.pdf (accessed March 17, 2010).

Moore, Adrian. “How a risk-based approach would focus resources on terrorists trying to bring down planes.” January 27, 2010. Reason Foundation. http://reason.org/news/show/1009342.html (accessed March 11, 2010).

Jackson, Brian, et al. “Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies,” RAND Corporations 2007. (http://www.rand.org/pubs/monographs/2007/RAND_MG481.pdf) (accessed February 19, 2010).

Jackson, Brian. “Technology Strategies for Homeland Security: Adaptation and Coevolution of Offense and Defense.” *Homeland Security Affairs Journal,* V, no. 1, January 2009. http://www.hsaj.org/?article=5.1.4 (accessed March 12, 2010).

Janis, Irving L. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd, rev. ed. (Boston: Houghton Mifflin, 1983), 9.

———. “Victims of Groupthink**.”** *Political Psychology* 12, no. 2, June 1991, 247–278.

Jehl, Douglas. The New Magic Bullet: Bureaucratic Imagination, *New York Times*. July 25, 2004. http://www.nytimes.com/2004/07/25/weekinreview/25jehl.html?pagewanted=1 (accessed March 22, 2010).

Johnson, Andrew, and Emily Dugan. “The inside story of the privileged student who embraced al-Qaida and tried to blow a transatlantic jet out of the sky – and the lessons for us all.” December 27, 2009, *The Independent*, http://www.independent.co.uk/news/world/americas/wealthy-quiet-unassuming-the-christmas-day-bomb-suspect-1851090.html (accessed January 14, 2010).

Johnson, Phillip M. “Effects of Groupthink on Tactical Decision-Making,” School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas.

Kaufmann, Keith. TSA Blog. March 4, 2008. http://www.tsa.gov/blog/2008/03/how-intelligence-drives-operations-at.html (accessed March 17, 2010).

Kerr, Bob. Combined Arms Center Public Affairs (TRADOC News Service, August 28, 2003) http://www-tradoc.monroe.army.mil/pao/people_portraits/wallace.htm (accessed March 1, 2010).

Kirkpatrick, Shelly, Shelley Asher, and Catherine Bott. “Staying One Step Ahead: Advancing Red Teaming Methodologies Through Innovation.” Arlington, VA: Homeland Security Institute, February 8, 2005, 4.

Laqueur, W. *No End to War: Terrorism in the Twenty-First Century.* New York, NY: Continuum International Publishing Group Inc. 2003.

Marcus, Leonard J., Barry C. Dorn, and Joseph M. Henderson. *Meta-Leadership and National Emergency Preparedness*, U.S. Centers for Disease Control and Prevention, 42.

Lieberman, Joseph. Senate Homeland Security and Governmental Affairs Committee, January 20, 2010. *Intelligence Reform: The Lessons and Implications of the Christmas Day attack.* http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=db07fd72-c631-42ea-a514-215127425e3a (accessed January 23, 2010).

Longbine, David. "Red Teaming: Past and Present, School of Advanced Military Studies," United states Army Command and General Staff College, Ft. Leavenworth, Kansas, 2008.

Lute, Jane Holly. Deputy Secretary Department of Homeland Security, testifying before U.S. House of Representatives Committee on Homeland Security, Flight 253: Learning Lessons from an Averted Tragedy, January 27, 2010. http://hsc.house.gov/SiteDocuments/20100127100900-30495.pdf (accessed February 12, 2010).

Luther, Nathan. "Bureaucracy: The Enemy Within." Proceedings. www.dacom.com/fighting.../B92%20Bureaucracy%20Within.doc (accessed March 17, 2010).

Malone, Timothy G., and Reagan E. Schaupp. "The 'Red Team' Forging a Well-Conceived Contingency Plan." *Aerospace Power Journal*, Summer 2002. ttp://www.airpower.maxwell.af.mil/airchronicles/apj/apj02/sum02/malone.html#malone (accessed March 17, 2010).

Mayerwitz, Scott. A Look at How Air Travel Has Changed and What You Now Need to Do at the Airport (January 6, 2010,). ABC News. http://abcnews.go.com/Travel/airline-security-today-changed-checkpoint-travels/story?id=9484884 (accessed February 15, 2010).

McGannon, Mike. Developing Red Team Tactics, Techniques and Procedures, *The Vanguard*, Spring 2005, 4.

Meehan, Michael K. "Red Teaming for Law Enforcement," *The Police Chief Magazine*, 1, http://policechiefmagazine.org/magazine/index.cfm?fuseaction=print_display&article_id=1111&issue_id=22007 (accessed March 2, 2009).

Miller, Gregory D. (2009). "Teaching About Terrorism: Lessons Learned at SWOTT." *Political Science & Politics 42,* October 2009, 773–779.

Nance, Malcolm. “How (Not) to Spot a Terrorist.” *Foreign Policy*, April 10, 2008. www.foreignpolicy.com/articles/2008/04/10/how_not_to_spot_a_terrorist? (accessed March 11, 2010).

Napolitano, Janet. “Secretary Napolitano to Discuss Ways to Bolster Global Aviation Security with International Partners in Mexico.” February 12, 2010. http://www.dhs.gov/ynews/releases/pr_1266006073168.shtm (accessed March 15, 2010).

National Commission on Terrorist Attacks. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). 2004. The 9/11 commission report: Final report of the National Commission on Terrorist Attacks upon the United States. New York: W.W. Norton.

National Research Council (U.S.). Committee on Science and Technology for Countering Terrorism. Panel on Transportation. Deterrence, protection, and preparation: the new transportation security imperative (Special report; 270) “Transportation Research Board, National Research Council.” ISBN 0-309-07710-9, http://onlinepubs.trb.org/onlinepubs/sr/sr270.pdf (accessed April 1, 2010).

New York Times. Umar Farouk Abdulmutallab, updated February 3, 2010. http://topics.nytimes.com/top/reference/timestopics/people/a/umar_farouk_abdulmutallab/index.html?inline=nyt-per (accessed April 1, 2010).

O’Brien, Miles. “Model for air travel security may be El Al,” September 26, 2001. CNN http://archives.cnn.com/2001/WORLD/meast/09/26/rec.el.al.security/ (accessed March 15, 2010).

Obama, Barak. Remarks from the President on strengthening intelligence and aviation security, January 7, 2010, http://www.whitehouse.gov/the-press-office/remarks-president-strengthening-intelligence-and-aviation-security (accessed March 10, 2010).

Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, Defense Science Board Task Force on the Role and Status of DoD Red teaming Activities, September 2003.

Patterson, Mark C., and Sam Jin. “Overcoming the Complexities of Wars.” *Knowledge: Official Safety Magazine*, U.S. Army. https://safety.army.mil/Knowledge_Online/Portals/february2010/Overcoming_the_Complexities_of_War.pdf (accessed March 17, 2010).

Poole, Robert, and James Carafano. Time to Rethink Airport Security, July 26, 2006, http://www.heritage.org/research/homelandsecurity/bg1955.cfm (accessed February 15, 2010).

Poole, Robert. Toward Risk-Based Aviation Security Policy, Discussion Paper No. 2008-23, November 2008, Joint Transport Research Centre.

———. The Case For Risk-Based Aviation Security Policy. *World Customs Journal* 3, no. 2, 2009, 4. http://www.worldcustomsjournal.org/media/wcj/-2009/2/WCJ_V3N2_Poole_(web).pdf (accessed March 14, 2010).

Ramos, Kelsey. *Do tightened airport security measures protect us or distract from the problem?* December 28, 2009, http://latimesblogs.latimes.com/comments_blog/2009/12/new-tightened-airport-security-measures-janet-napolitano-northwest-airlines-flight.html , accessed 14 January 2010.

Rampell, Catherine. Ex-employee says FAA warned before 9/11_ *USA Today*, www.usatoday.com/news/washington/2006-11-23-whistle-blower-faa_x.htm , accessed January 14, 2010.

University of Foreign Military and Cultural Studies, Red Team Handbook, ver. IV, October 12, 2007. Distribution Restriction: (Draft) Distribution is limited to UFMCS Faculty, Red Team course graduates and adjunct professors.

Red Teaming for Program Managers, Sandia National Laboratories. http://idart.sandia.gov/methodology/RT4PM.html (assessed March 17, 2010).

Report to the President of the United States, March 31, 2005, The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, in Red Team IV Handbook (Draft), 170.

Robinson, Virgil. History of the Devil's Advocate, September 2008, http://possibilityadvocate.ning.com/notes/History_of_the_Devil's_Advocate (accessed January 11, 2010.

Ross, Brian and Esposito, Richard, ABC News, 28 Dec 2009, http://abcnews.go.com/Blotter/abdulmutallab-yemen-northwest-flight-253-terror-suspect/story?id=9430536 (accessed January 14, 2010.

Rugy, Veronica, TSA Disaster, Leave it to the government, *National Review* Online, May 5, 2005, http://old.nationalreview.com/comment/de_rugy200505050751.asp (accessed March 8, 2010).

Sandoz, John F. "Red Teaming: A Means to Military Transformation, Institute for Defense Analyses." Paper P-3580, Log H 00_002905, January 2001, 1.

Schwenk, Charles R. "Devil's Advocacy in Managerial Decisions," *Journal of Management Studies* 1, no. 2, April 1984, 168. http://libproxy.nps.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=4554857&site=ehost-live&scope=site (accessed February 9, 2010).

Simon, Bob. "The Safest Airline, A Secure Example Set By Israel's El Al." August 21, 2002. 60 Minutes, CBS News. http://www.cbsnews.com/stories/2002/01/15/60II/main324476.shtml (accessed March 15, 2010).

Sinnreich, Richard. Red Team Insights from Army Wargaming, Defense Adaptive Red Team Working Paper #02-3, September 2002, 1.

Steele, Robert David. TAKEDOWN: The Asymmetric Threat to the Nation. June 22, 1998. Joint Forces Quarterly (Winter 1998–99). www.defensedaily.com/reports/takedown.htm. accessed March 17, 2010.

Sullivan, Eileen. CQ Homeland Security – Local Response. CQ Today. June 13, 2007. http://public.cq.com/docs/hs/hsnews110-000002531281.html (accessed March 17, 2010).

Taper, Jake. Hoekstra on Underwear Bomber: "We Missed Him at Every Step." ABC News. http://blogs.abcnews.com/politicalpunch/2009/12/hoekstra-on-underwear-bomber-we-missed-him-at-every-step.html (accessed March 11, 2010.)

Teaming Methodologies through Innovation" (Arlington, VA: Homeland Security Institute, 2005), 1.

Tellis, Winston. "Introduction to Case Study," *The Qualitative Report*, 3, no. 2, July 1997 (http://www.nova.edu/ssss/QR/QR3-2/tellis1.html) accessed 7 February 7, 2010.

"Top Ten Challenges Facing the Next Secretary of Homeland Security," Homeland Security Advisory Council, September 11, 2008, 12 http://www.dhs.gov/xlibrary/assets/hsac_dhs_top_10_challenges_report.pdf (accessed February 1, 2009).

Transportation Research Board, Deterrence, Protection, and Preparation.

Transportation Security Administration. Mission Statement, http://www.tsa.gov/who_we_are/mission.shtm (accessed December 12, 2009).

———. Layered Security: What we do. http://www.tsa.gov/what_we_do/layers/index.shtm (accessed March 8, 2010).

———. Travel Assistant, http://www.tsa.gov/travelers/airtravel/screening/index.shtm (accessed February 15, 2010).

———. VIPR Teams Enhance Security at Major Local Transportation Facilities, June 20, 2007. http://www.tsa.gov/press/happenings/vipr_blockisland.shtm (accessed March 22, 2010).

Treverton, Gregory F. *The Next Steps in Reshaping Intelligence*. Santa Monica, CA: RAND Corporation. ISBN: 0-8330-3857-5, http://www.rand.org/ (accessed March 22, 2010).

Tuchman, B. *The Guns of August.* New York, NY: Macmillan Publishing Co., Inc., 1962.

U.S. Army Field Manual 5-0, 2–8.

U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008–2013, 3. http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf (accessed March 15, 2010).

U.S. Homeland Security (Government and Private) Market Outlook – 2007–2011. Homeland Security Research, January 2007

United States General Accounting Office. Cathleen A. Berrick, Director Homeland Security and Justice Issues, Testimony before the Committee on Commerce, Science and Transportation, U.S. Senate. Aviation Security Efforts to Measure Effectiveness and Address Challenges. November 5, 2003. GAO-04-232T, 1.

———. Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts, October 31, 2001, Statement of Raymond J. Decker, Director, Defense Capabilities and Management GAO-02-208T http://www.gao.gov/new.items/d02208t.pdf (accessed March 17, 2010).

———. GAO Report to Congressional Requesters: Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges, GAO-10-128, October 2009, 1.

———. Report to the Chairman, Committee on Homeland Security, House of Representatives; Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests. August 2008, GAO-08-958.

University of Foreign Military and Cultural Studies (UFMCS). Red Team Handbook, V4, October 12, 2007, 10.

Walker, Christopher. “Air security: rest of world needs to learn from El Al.” *First Post*. January 21, 2010. http://www.thefirstpost.co.uk/58471,news-comment,news-politics,air-security-rest-of-world-needs-to-learn-from-el-al (accessed March 15, 2010).

Whitehouse. Summary of Whitehouse review of the December 25, 2009 attempted terrorist attack. http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf (accessed March 12, 2010).

Williamson, Murray. Red Teaming: Its Contributions to Past Military Effectiveness (McLean, VA: Hicks and Associates, September 2002), 58.

Wirtz, James J. “Miscalculation, Surprise and American Intelligence After the Cold War,” *International Journal of Intelligence and Counterintelligence* 5, no. 1, 1991, 5. Intel Publishing Group, Inc.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California